



U.S. Department of Agriculture

---



Office of Inspector General  
Financial and IT Operations

## **Audit Report**

### **Review of Rural Development's Information Technology Resources Security**

Report No. 85099-4-FM  
March 2004

---



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL



Washington D.C. 20250

DATE: MAR 31 2004

REPLY TO  
ATTN OF: 85099-4-FM

SUBJECT: Review of Rural Development's Information Technology Resources Security

TO: Gilbert Gonzalez  
Deputy Under Secretary  
Rural Development

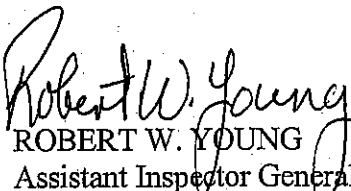
ATTN: John Purcell  
Director, Financial Management Division  
Operations and Management

This report presents the results of our audit of Rural Development's Information Technology Resources Security. The report identified serious weaknesses in Rural Development's ability to protect its critical information technology resources.

Based on your response, we were able to reach management decision concerning Recommendation No. 1. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer. To reach management decision on the remaining recommendations, we need additional information, detailed corrective action plans, and timeframes for implementation. Please refer to the OIG Position sections of the report for specific details.

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 a maximum of 6 months from report issuance.

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

  
ROBERT W. YOUNG  
Assistant Inspector General  
for Audit

# Executive Summary

## Review of Rural Development's Information Technology Resources Security

---

### Results in Brief

This audit was performed as a followup review to our prior audit<sup>1</sup> of Rural Development information technology (IT) controls. That audit disclosed, and we continue to find, material weaknesses in Rural Development's ability to effectively ensure the integrity and confidentiality of its IT resources. We believe the major cause of these material weaknesses is that the Chief Information Officer (CIO) and Information System Security Program Manager are not properly aligned within the organizational structure to effectively implement a strong security program. Further, exhibit A of this report shows that Rural Development has had a long history of reacting to IT-related audit findings rather than instituting controls to address the systemic weaknesses in its internal control structure. As a result, there is ineffective oversight and management of its IT resources that unnecessarily expose Rural Development's critical loan portfolio data to the risk of disclosure, modification, or deletion.

We also continue to find that Rural Development is not in compliance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and Federal Information Security Management Act (FISMA) requirements. Despite some actions to initiate the preparation of security plans, risk assessments, and certifications and accreditations of its major application and support systems, Rural Development has not completed these tasks, and in some cases not completed in accordance with OMB guidelines. These documents are the foundation of a strong security program and without them Rural Development cannot be assured that all the necessary controls are in place and functioning as intended.

Material weaknesses persist in Rural Development's ability to effectively control access to its sensitive systems and data. Rural Development has not established and implemented effective internal controls to ensure that (1) user identifications belonging to former employees are removed timely, (2) users have only the access needed to perform their job functions, (3) remote accesses to Rural Development resources are properly managed and secured, and (4) password settings conform to National Institute of Standards and Technology (NIST) guidance. While Rural Development had instituted a process to circulate user lists to responsible management officials to verify access, the security staff did not include all of Rural Development systems or the level of access that each user had. Without all of the necessary data, this control is incomplete and ineffective. Without effective logical access

---

<sup>1</sup> Audit Report No. 85099-2-FM, "Security Over Rural Development's Information Technology Resources Needs Improvement," dated August 5, 2002.

controls, Rural Development's critical loan data is at risk of disclosure, modification, or deletion.

We also continued to identify numerous vulnerabilities in Rural Development's systems, including some that remained despite Rural Development's knowledge of the vulnerabilities through its contractors in 1997, and reported by the Office of Inspector General in 1999 and again in 2001. Rural Development has not taken adequate corrective actions to correct known vulnerabilities, or established effective controls to ensure that vulnerabilities are identified and corrected timely. As a result, Rural Development's systems are unnecessarily vulnerable to exploitation.

Rural Development was not following its own policies<sup>2</sup> for identifying, selecting, installing, and modifying software. Further, those same policies did not conform to departmental, NIST, and OMB guidance regarding change controls and segregation of duties. Hence, we were unable to validate that system software changes, (1) received proper authorization, (2) were supported by change request documents, (3) were properly tested and test results approved, or (4) were properly monitored while being moved into the production environment. Rural Development officials were unable to provide us an explanation for this internal control weakness, but agreed that they needed to conform to proper change control procedures.

Finally, Rural Development had not ensured that all IT security controls were in place at its State and county offices. Our fieldwork in selected State and county offices across the country disclosed that Rural Development had not established controls to ensure that those offices had adequately maintained contingency planning documents, physically secured IT equipment, and ensured that all of its field employees received security awareness training. As a result, Rural Development cannot be assured that its IT resources are properly secured at its remote offices.

Despite some of its actions, it is apparent that Rural Development has not addressed the underlying cause of its poor information security by instituting a framework for proactively managing the information security risks associated with its operations. Instead, Rural Development has reacted to individual audit findings as they were reported, with little ongoing attention to the systemic causes of control weaknesses. The Department CIO assessed Rural Development's security program at an intermediate stage noting the policies have been designed, implemented, and at least 50 percent had been tested. While we agree that Rural Development has numerous policies in place that if implemented could improve Rural Development's security posture, our detailed testing shows that Rural Development has not

---

<sup>2</sup> "Rural Development Application Information Systems Support Handbook," dated May 1997.

implemented all of its policies, or in many cases, not implemented them effectively.

**Recommendation  
In Brief**

We recommended that Rural Development:

- Implement interim measures to ensure that security controls, including those recommended elsewhere in this report, are implemented and effectively carried out;
- address weaknesses in its audit resolution process;
- establish plans of action with specific timeframes for compliance with OMB Circular A-130 and FISMA;
- establish plans of action with specific timeframes to address the systemic weaknesses in its ability to effectively manage logical access and vulnerability mitigation processes;
- strengthen controls over application change authorization, testing, and implementation; and
- establish a timeline of corrective actions with specific timeframes for addressing the State and county office IT weaknesses addressed in this report.

**Agency Response**

Rural Development agreed with the findings and recommendations in the report and has initiated corrective actions.

**OIG Position**

We concurred with Rural Development's proposed corrective actions to most of the recommendations. However, we need additional information or timeframes to enable us to reach management decision.

## ***Abbreviations Used in This Report***

---

ADP	Automated Data Processing
CCE	Common Computing Environment
CIO	Chief Information Officer
DCIO	Deputy Chief Information Officer
DM	Department Manual
DR	Departmental Regulation
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers' Financial Integrity Act
FmHA	Farmers' Home Administration
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
ID	Identification (i.e., user ID or account on a system)
ISSPM	Information System Security Program Manager
IT	Information Technology
ITWG	Information Technology Working Group
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
POA&M	Plan of Action and Milestones
RD	Rural Development
SP	Special Publication
USDA	United States Department of Agriculture

# Table of Contents

---

Executive Summary .....	i
Abbreviations Used in This Report.....	iv
Background and Objectives.....	1
Findings and Recommendations.....	3
<b>Section 1. Security Management and Compliance with OMB IT Security Requirements .....</b>	<b>3</b>
Finding 1 Security Management Structure has Remained Ineffective Despite Prior Recommendations .....	3
Recommendation No. 1.....	5
Recommendation No. 2.....	5
Finding 2 Actions Needed to Ensure Compliance with OMB Circular A-130 and FISMA.....	6
Recommendation No. 3.....	12
Recommendation No. 4.....	12
<b>Section 2. Ineffective Management of Access Controls and System Vulnerabilities .....</b>	<b>14</b>
Finding 3 Rural Development does not Effectively Manage Access Controls .....	14
Recommendation No. 5.....	16
Finding 4 Rural Development is not Vigilant in Identifying and Correcting Identified System Vulnerabilities .....	16
Recommendation No. 6.....	19
Recommendation No. 7.....	19
<b>Section 3. Application Change Controls .....</b>	<b>21</b>
Finding 5 Application Change Controls Need Strengthening .....	21
Recommendation No. 8.....	23
Recommendation No. 9.....	24
Recommendation No. 10.....	24
<b>Section 4. Field Office IT Controls .....</b>	<b>26</b>
Finding 6 IT Controls at State and County Offices Need Strengthening .....	26
Recommendation No. 11.....	27
Scope and Methodology.....	29
General Comments .....	30

**Exhibit A – History of OIG Evaluations of Rural Development IT Controls..... 31**  
**Exhibit B – Agency Response ..... 32**



# Background and Objectives

---

## Background

Information security, improving the overall management of information technology (IT) resources, and the transition to electronic business (e-Government), have emerged as top priorities within the U.S. Department of Agriculture (USDA). As technology has enhanced the ability to share information instantaneously among computers and networks, it has also made organizations more vulnerable to unlawful and destructive penetration and disruptions. This environment poses a threat to the sensitive and critical operations of Rural Development, unless aggressive actions are taken to secure its systems.

Various laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995. Responsibilities regarding information security were reemphasized in the Clinger-Cohen Act of 1997 and Presidential Decision Directive (PDD) 63.<sup>3</sup> On December 17, 2002, the President signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. The National Institute of Standards and Technology (NIST)<sup>4</sup> has issued numerous Federal Information Processing Standards, as well as a comprehensive description of basic concepts and techniques entitled, "An Introduction to Computer Security: The NIST Handbook," Special Publication (SP) 800-12, October 1995.

Finally, Departmental Manual (DM) 3140-1<sup>5</sup> and Office of the Chief Information Officer guidance also provides standards, guidelines, and procedures for the development and administration of automated data processing (ADP) security programs mandated by Departmental Regulations (DR).

Rural Development programs consist of a variety of loan, loan guarantee, and grant programs plus technical assistance in the areas of business and industry, cooperative development, rural housing, community facilities, water and waste disposal, electrification, and telecommunications. Rural Development programs are administered through four services; the Rural Utilities Service, the Rural Business-Cooperative Service, the Office of Community Development, and the Rural Housing Service.

---

<sup>3</sup> PDD 63, "Policy on Critical Infrastructure Protection."

<sup>4</sup> The Computer Security Act of 1987 assigned NIST primary responsibility for developing technical standards and providing related guidance. Their responsibilities were reemphasized in the Clinger-Cohen Act of 1997.

<sup>5</sup> DM 3140-1, "Management ADP Security Manual," Part 1 of 8, Section 1, July 19, 1984.

Rural Development programs are delivered through a National office in Washington D.C., 47 State offices, and 909 National and district offices. The mission is supported by program staffs and a Centralized Servicing Center located in St. Louis, Missouri, which services the direct single-family housing portfolio.

## **Objectives**

The audit objectives were:

- To assess the corrective action taken by Rural Development on previously identified control weaknesses to determine the adequacy of general controls over Rural Development's information systems.
- To determine if adequate logical access controls exist to protect resources against unauthorized modification, disclosure, loss, or impairment.
- To evaluate the controls over the modification of application software programs to ensure that only authorized modifications are implemented.
- To determine the adequacy of controls over access to and modification of system software.

# Findings and Recommendations

## Section 1. Security Management and Compliance with OMB IT Security Requirements

---

The Office of Inspector General (OIG) can provide periodic independent assessments of Rural Development operations, ultimately it is Rural Development management's responsibility for ensuring that internal controls, including information security controls, are adequate and effectively implemented on an ongoing basis. It is apparent that Rural Development has not addressed the underlying cause of its poor information security by instituting a framework for proactively managing the information security risks associated with its operations. Instead, Rural Development has reacted to individual audit findings as they were reported, with little ongoing attention to the systemic causes of control weaknesses. The integrity, confidentiality, and availability of Rural Development's data remains at risk unless significant measures are taken to proactively address IT security weaknesses.

---

### Finding 1

#### **Security Management Structure has Remained Ineffective Despite Prior Recommendations**

Rural Development's Chief Information Officer (CIO) and Information System Security Program Manager (ISSPM) are not assigned to a level within Rural Development's organizational structure to effectively implement a strong security program. Despite our prior recommendation and the results of an independent assessment into this issue, Rural Development has not taken adequate steps to remedy this issue. As a result, there is ineffective oversight and management of IT resources, many of which are detailed in the remaining findings in this report.

DR 3140-1<sup>6</sup> requires agency administrators to ensure that ISSPMs are assigned to a level within the organization that can independently report to the appropriate program officials. The ISSPM must be able to enforce the security policies across the entire agency's programs. DR 3140-1 also requires that agency administrators ensure that the security program function is properly staffed and resources are allocated to allow effective implementation and continuance of a comprehensive and proactive agency security program.

---

<sup>6</sup> DR 3140-1, "USDA Systems Security Policy," May 15, 1996.

As a result of our prior audit,<sup>7</sup> Rural Development agreed to contract for a review of its IT organizational structure to determine the appropriate structure to effectively carry out a strong security program. The results of that study concluded that the management structure was, as we reported, ineffective in its ability to implement a strong security program. However, as of September 2003, no significant organizational changes have occurred.

Rural Development's management informed us of its plans to reorganize most of its security staff along with proposed changes to the management of the Common Computing Environment (CCE).<sup>8</sup> However, we were informed that Congress did not fund the proposed changes for fiscal year 2004, and that it was uncertain whether the funding would be received in fiscal year 2005. Due to the size, decentralized management, involvement in the multi-agency CCE initiative, and the seriousness of the issues we again raise in this report, we believe that Rural Development needs to implement significant interim measures to establish clear lines of authority and implement accountability controls to ensure that its security program is adequately implemented and managed.

#### Audit Resolution

The issues brought forth once again in this report (see exhibit A which summarizes our audit results since 1988); indicate that Rural Development has had a long history of unsatisfactorily addressing IT-related weaknesses in a timely manner. Further, management decision had not been reached on 12<sup>9</sup> of 20 recommendations in our prior audit report. In addition, of the eight recommendations where management decision had been reached, Rural Development had not taken effective actions to correct the systemic internal control issues we identified.

The Federal Managers' Financial Integrity Act (FMFIA) requires agencies to comply with the General Accounting Office (GAO) issued standards of internal controls. One of those standards requires that agencies establish policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved, and that the audit resolution process is not complete until actions have been taken to correct identified deficiencies.

To comply with Federal internal control standards, Rural Development needs to implement effective controls to ensure that (1) audit issues are resolved by addressing the cause of the weakness, and (2) corrective action taken is adequate and completed timely.

---

<sup>7</sup> Audit Report No. 85099-2-FM, "Security Over Rural Development's Information Technology Resources Needs Improvement," dated August 5, 2002.

<sup>8</sup> Rural Development is one of three agencies that participate in the CCE.

<sup>9</sup> At the time of our fieldwork, management decision was reached on only eight recommendations. Since our fieldwork ended, we have reached management decision on an additional seven recommendations.

## Recommendation No. 1

Until funding is obtained to implement broader organizational changes, implement interim measures with specific timeframes for achievement to ensure that security controls, including those recommended elsewhere in this report, are implemented and effectively carried out.

**Agency Response.** Effective January 12, 2004, the Information Systems Security Staff (ISSS) was reassigned to report directly to the Deputy Chief Information Officer (DCIO). This emphasizes the level of importance current management places on security issues and frees the security staff from the normal internal debates on prioritization by establishing security as always having the highest CIO priority and allows the ISSS to effectively implement the Agency's Information Systems Security Program (ISSP).

In addition, an onsite security position was established in the Washington, D.C. office as the liaison with ISSS on Washington, D.C. related security issues. Responsibilities of this position include coordinating and reviewing the general support system or major application risk assessments, security plans, and mitigation efforts; assisting in identifying, researching, mitigating, and reporting on security-related information pertaining to incidents and acknowledged or suspected weaknesses and vulnerabilities in the agency's information systems; and assisting in gathering, resolving, and reporting on Departmental, oversight agency, and agency internal and external audit information and mitigation efforts.

Weekly meetings were initiated in December 2003 between the Washington, D.C. liaison and the ISSS to discuss open security related issues. A tracking spreadsheet has been created which includes the issue, the date it was raised, the responsible entity, and the status. This has greatly improved the standardization of security throughout Rural Development and provides a means of communication of issues from both perspectives, the Washington, D.C. community and ISSS.

**OIG Position.** Management Decision has been reached on this recommendation.

## Recommendation No. 2

Rural Development needs to establish a second-party review within its management decision process relating to IT recommendations to ensure that the corrective actions proposed address the systemic cause of the audit finding. Further, followup needs to be done at the National office level to ensure corrective actions have been effectively implemented before final action is forwarded to the Office of the Chief Financial Officer (OCFO).

**Agency Response.** Audit Responses are prepared by the Financial Management Systems Branch representatives based on information provided by subject matter experts, for example the ISSS staff for security findings. Once formulated, the subject matter experts, the DCIO, the CIO, and the Deputy Administrator for Operations and Management review the proposed corrective actions prior to submission to OIG and/or to the Office of the Chief Financial Officer.

A project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team, which includes the Information Systems Security Program Manager (ISSPM) and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for the corrective actions, and to review the status of the proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

**OIG Position.** We agree that Rural Development's project plan to track outstanding audit issues will go a long way toward improving followup on audit issues; however, as our report identifies, Rural Development has had a long history of not ensuring that corrective actions are fully implemented once management decision has been reached. In order to reach management decision, Rural Development needs to establish a policy and internal controls to ensure that management decision actions are implemented and that final action was complete before closure requests are sent to the OCFO. Further, Rural Development needs to provide a date when this policy and controls are put in place.

---

**Finding 2**

**Actions Needed to Ensure Compliance with OMB Circular A-130 and FISMA**

Rural Development needs to establish effective controls to ensure compliance with the Office of Management and Budget (OMB) Circular A-130 and FISMA requirements. We concluded that it is a lack of an effective management structure and demonstrated commitment to compliance that makes this weakness an outstanding issue. As a result, Rural Development cannot be assured that all the necessary controls needed to manage its security program are in place and operating effectively.

OMB Circular A-130<sup>10</sup> established a minimum set of controls for agencies' automated information security programs, including security planning, periodic review of security controls, and management authorization of systems to process information. Comprehensive guidance on planning and managing an entity-wide security program has been established by NIST<sup>11</sup> addressing security-related management, operational, and technical controls. Further, PDD 63<sup>12</sup> requires agencies to assess the risks to their networks and establish a plan to mitigate the identified risks.

### Risk Assessments

Rural Development has still not completed the required risk assessments on its major applications as required by OMB Circular A-130, NIST SP 800-18,<sup>13</sup> PDD 63, and its own policy.<sup>14</sup> 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. Until these risk assessments are completed, Rural Development cannot be assured that all the risks attributable to its mission-critical systems have been considered and that appropriate steps have been taken to mitigate these risks.

### Security Plans

OMB Circular A-130 states that all general support systems contain some sensitive information that requires protection to assure its integrity, availability, or confidentiality; and therefore, require security plans. Additionally, Rural Development's Data Security Manual, dated February 16, 2000, requires security plans for all computer systems that process sensitive data. Further, NIST and OCIO guidance on the preparation of security plans identifies a 'system' by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must be under the same direct management control, have the same function or mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.

Rural Development had not prepared security plans for its general support systems in Washington, D.C., St. Louis, Missouri, or its web farm. This was

---

<sup>10</sup> OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.

<sup>11</sup> NIST SP 800-12, "An introduction to Computer Security: The NIST handbook," dated October 1995.

<sup>12</sup> PDD 63, "Policy on Critical Infrastructure Protection," dated May 22, 1988.

<sup>13</sup> NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems," dated December 1998.

<sup>14</sup> RD Instruction 2006-2, "Information Systems Security," dated July 16, 1997, Section 2006.1260 (e).

also reported in our prior audit. Further, we found that while Rural Development prepared security plans for some of its applications, it had combined systems that did not have the same operating characteristics or operating environment into a single security plan. Our discussions with an official at the Department's Office of the Chief Information Officer (OCIO) found that while it may be appropriate to combine systems when performing other reviews, Rural Development should prepare separate security plans for each major application and general support system.

### Disaster Recovery Planning

Rural Development is not fully prepared in the event of a disaster or major disruption. While Rural Development does participate in disaster recovery hot site tests initiated by Department data centers, Rural Development has not identified all the critical data it needs to fully recover, nor does it confirm with data center personnel that the appropriate data is being backed up. Further, Rural Development has not completed disaster recovery plans for its major network operations in St. Louis, Missouri, or Washington, D.C.

We found that Rural Development has over 90,000 data files consisting of program code and data. The results of a hot site test performed in early calendar year 2003 disclosed that not all the tests could be fully implemented because not all data files had been identified, and therefore not taken to the hot site testing facility. While the data center personnel actually perform backup and restore procedures on Rural Development data, it is Rural Development's responsibility to identify those data files that need to be backed up, and receive assurance from the data center that backups are properly completed.

We also found that Rural Development does not have disaster recovery plans<sup>15</sup> for its general support systems or major applications, despite its own policy that all National and St. Louis office heads be responsible for preparing them. Further, at the time of our review Rural Development had not established milestones with estimated completion dates for the preparation of these plans. Without contingency plans in place, Rural Development cannot be assured that vital automated information needed to support its business processes will be able to operate effectively without excessive disruption.

### Background Investigations

Federal Law<sup>16</sup> and OMB Circular A-130 require that persons in positions of public trust and those who are authorized to bypass significant technical and

---

<sup>15</sup> "Rural Development Data Security Manual," Section 13.0, dated February 16, 2000.

<sup>16</sup> Title 5, Code of Federal Regulations, Section 731.106



operational security controls have periodic background investigations. DM 3140 requires personnel, including contractors, working in the IT environment to have proper personnel security clearances. This requirement is also stated in Rural Development's data security manual<sup>17</sup> and employee security handbook.<sup>18</sup>

Despite the significant numbers of security personnel we reported in our last report as not having had adequate background investigations, we again found the following:

- Of the 10 contractors working as security officers, 7 did not have a security clearance. Additionally, we found Rural Development's CIO had not had a background investigation completed. Finally, we identified four security staff with background investigations more than 5 years old, including Rural Development's ISSPM whose last background investigation was performed in 1989.
- Of the 109 Rural Development employees and contractors we reviewed with security authority at a Department data center, 55 had not had background investigations. In addition, we found an additional 23 of the 109 had background investigations more than 5 years old, with 3 dating back to the 1970s.
- Of the 16 system administrators we identified, 11 had not received security clearances, and an additional 3 system administrators had security clearances over 5 years old.
- Of the 39 security points of contact, who act as liaisons with the security staff in various agency branches and approve and review access privileges, we identified 17 that had not had background investigations performed and an additional 5 that had background investigations over 5 years old.

#### System Certification and Accreditation

Rural Development had not ensured that any of its 15<sup>19</sup> major applications were certified and accredited in accordance with OMB Circular A-130. OMB states that agencies should perform an independent review of the security controls in each application at least every 3 years. Further, Rural

---

<sup>17</sup> "Rural Development Data Security Manual," Section 12.1, dated February 16, 2000.

<sup>18</sup> "Information Systems Security Handbook," Section 3.2.3b, dated March 10, 2003.

<sup>19</sup> During our prior audit, Rural Development reported to us that it had only 14 major applications. Since that audit, Rural Development has re-categorized some of its applications to meet Department and OMB definition of major applications. Rural Development now reports a total of 15 applications that are critical to its operations or that maintain Privacy Act or other sensitive data. The scope of our review did not entail ensuring that Rural Development properly identified its systems, but rather tested whether Rural Development had conducted system certifications and accreditations for the major applications it identified.

Development's own policy<sup>20</sup> requires an agency official to certify applications meet all applicable Federal requirements, and that all Information System Security requirements and controls are adequate before allowing the application into production and every 3 years thereafter. Without adequate certification and accreditation of Rural Development's mission-critical systems, Rural Development cannot be assured that adequate security controls have been established for these systems and controls are operating effectively. Rural Development, with the help of the Department OCIO, has begun the process to contract for these certifications and accreditations.

### Incident Response Procedures

Rural Development has still not strengthened controls to adequately track security incidents and ensure that adequate corrective actions are taken to prevent recurrence. In our prior report, we found that despite established policies both at the Department<sup>21</sup> and agency<sup>22</sup> level, Rural Development staff were not preparing incident reports, but merely responding to Department OCIO e-mail notification of a security incident. Further, our review showed that Rural Development maintained documentation for only 13 of the 28 incidents reported by the Department OCIO during calendar year 2001.

During our current review we found no noticeable improvement in Rural Development's ability to timely and adequately respond to security incidents. For instance, the Department OCIO notified Rural Development three times within a 3-month period that one of its systems in a State office should be taken offline and patched to correct a known system vulnerability. In another instance, the Department OCIO intrusion detection system identified a possible backdoor on one of Rural Development's systems. Rural Development closed the incident because it could not locate the Transmission Control Protocol/Internet Protocol address that OCIO reported. No further actions were taken on this incident and no other documentation was maintained.

### Plans of Action and Milestones (POA&M)

FISMA permanently reauthorized the framework outlined in GISRA. This Act requires agencies to prepare POA&Ms to track IT weaknesses and the milestones completed toward mitigating them. OMB Memorandum 02-01, dated October 17, 2001, outlines specific reporting requirements for the POA&Ms, including providing enough specifics on the weakness to trace it

<sup>20</sup> "Data Security Manual," Section 6.3, dated February 16, 2000

<sup>21</sup> "Cyber Security Manual 3500," Chapter 1, dated October 25, 2001.

<sup>22</sup> "Data Security Manual," Section 12.5, dated February 16, 2000.

back to a GAO or OIG report or internal review, the source of the weakness, and specific actions that need to be taken and the related cost of those actions.

Our review of Rural Development's POA&Ms showed that it was not a reliable management tool to track weaknesses and ensure corrective action was complete. For example, weaknesses identified by Rural Development were broad in nature, such as operational controls, security program and policy, and access controls. The actual weaknesses within these areas were not identified; making it virtually impossible to trace these weaknesses back to our prior report or another assessment. Further, Rural Development did not develop a separate POA&M for every program and system for which weaknesses were identified as required by OMB. Instead, Rural Development combined all weaknesses found in major applications into a single application POA&M.

Also, Rural Development did not include a completion date for the weaknesses or milestones identified. An estimated completion date provides a roadmap for continuous agency security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool for agency officials, Inspectors General, and OMB.

Per OMB, a milestone will identify specific requirements to correct an identified weakness. Many of the milestones reported by Rural Development did not identify specific requirements to correct an identified weakness. Some milestones that Rural Development listed were day-to-day tasks of the security office. For example, the June POA&M prepared by Rural Development identified gathering requested documents for OIG and GAO auditors as a completed milestone. This "milestone" does not identify a specific requirement to correct an identified weakness, but is a task in the day-to-day operation of the security staff. Additionally, in other instances, each step within a milestone (sub-milestones) were broken out and counted as an individual milestone. Both of these practices do not identify true milestones, but serve merely to inflate the numbers of completed milestones reported. Of the 381 total milestones reported as complete by Rural Development in the June POA&M submission, OIG identified 157 milestones that were not true milestones by OMB's definition.

Further, Rural Development inaccurately reported milestones as completed when they were merely merged with other milestones, or moved to a different POA&M. For example, in the March POA&M Status Update submitted by Rural Development, 123 of the completed 141 milestones reported by Rural Development were reported as complete when they were merely moved to either the application POA&M or the POA&M maintained by another agency.

While Rural Development has reported a total of 381 completed milestones as of June 2003, OIG identified only 43 that met the OMB definition of a milestone and had been completed. To ensure that the POA&M becomes an effective management tool as OMB intended, Rural Development needs to establish controls to ensure that the POA&M is completed per OMB instructions.

### **Recommendation No. 3**

Establish a plan of action with specific timeframes and allocate appropriate resources to establish policies and controls to ensure compliance with OMB Circular A-130 and FISMA.

**Agency Response.** Rural Development is in the midst of certification and accreditation of its major applications and general support system in accordance with OMB Circular A-130. Certification and accreditation activities performed during the first quarter of Fiscal Year 2004 were primarily preparatory and planning oriented. Tools were created and refined for guiding and streamlining certification and accreditation efforts including templates for performing privacy impact assessments, secure features users guides, and trusted facilities manuals.

The finding and recommendation in OIG Report 85099-2-FM, as well as in this report are very broad. Rural Development believes that by concentrating on the certification and accreditation, disaster recovery plan, and FISMA compliance while addressing access control and other outstanding audit issues, we will have come a long way to bringing our ISSP into compliance with OMB Circular A-130.

**OIG Position.** We agree that the certification and accreditation process will improve Rural Development's compliance with many, but not all, of the OMB Circular A-130 and FISMA requirements. The OMB Circular and requirements of FISMA are not all encompassing and serve as a foundation for a strong security program. Based on the pervasiveness of security program weaknesses in this and our prior audit, we believe Rural Development needs to implement explicit controls to ensure that they obtain and maintain compliance with OMB Circular A-130 and FISMA.

### **Recommendation No. 4**

Establish controls over the POA&M reporting process, including a second party review, to ensure that weaknesses are properly reported and that milestones reflect effective and measurable actions toward completion of the weakness.

**Agency Response.** The POA&M update was reformatted to conform to recently released Office of Management and Budget/OCIO-CS guidelines regarding the FISMA and the weaknesses and vulnerabilities identified during the analyses of the Fiscal Year 2003 FISMA submission. Existing and newly defined milestones will be integrated into appropriate POA&M's for the overall ISSP and each major application and general support system.

Audit resolution information from the project plan is included in the POA&M. Quarterly status reports, including an executive summary, are submitted to the OCIO-CS. Prior to submission to the OCIO-CS, the executive summary is reviewed and approved by the DCIO, the CIO, and the Deputy Administrator for Operations and Management. The Rural Development program administrators are provided copies of the quarterly POA&M status reports.

**OIG Position.** We agree with Rural Development's actions to reformat its POA&M to conform to OMB guidelines; however, the intent of the recommendation was to improve controls to ensure complete and accurate reporting of deficiencies. In order to reach management decision, Rural Development needs to provide us with specific controls that it will implement to ensure the POA&M process is complete and accurate.

## **Section 2. Ineffective Management of Access Controls and System Vulnerabilities**

---

Rural Development relies on computer-based information systems to carry out agency programs, manage its resources, and report financial statement data. The reliability of its systems is critical to Rural Development meeting its mission. Logical access controls should provide reasonable assurance that critical resources are protected against unauthorized modification, disclosure, loss, or impairment. Further, timely identification and mitigation of system vulnerabilities on Rural Development's network resources help ensure that its critical IT resources are protected from possible malicious attacks from both internal and external threats. Rural Development must implement and enforce sound access control, vulnerability assessments, and mitigation of vulnerabilities identified to ensure the integrity, confidentiality, and availability of the data maintained on its systems.

---

### **Finding 3**

#### **Rural Development does not Effectively Manage Access Controls**

Material weaknesses persist in Rural Development's ability to effectively control access to its sensitive systems and data. Rural Development has not established and implemented effective internal controls to ensure that (1) user identifications (ID) belonging to former employees are timely removed, (2) users have only the access needed to perform their job functions, (3) remote access to Rural Development resources are properly managed and secured, and (4) password settings conform to NIST guidance. Without effective logical access controls, Rural Development's critical loan data is at risk of disclosure, modification, or deletion.

DM 3140-1.6<sup>23</sup> 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 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. 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.

---

<sup>23</sup> DM 3140-1.6, "Management ADP Security Manual," part 6 of 8, Appendix D, Section 4.a.

Despite raising this issue in our prior audit, 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 Rural Development security staff did not include all Rural Development applications and did not instruct managers how to interpret the system-generated reports, which can be difficult to understand. The following illustrate the types of weaknesses we found:

- In one of Rural Development's networks with 706 user accounts, we identified 341 accounts that had been dormant for over 90 days. Of those 341 accounts, only 26 accounts had been disabled. Further, 162 of the 341 had not been used within the past year and an additional 106 had never been used. In this same network, we found that passwords were set to never expire, 533 of the 706 users had not changed their account passwords in over 60 days, 356 of which had not changed their passwords in over 1 year. Finally, this same network allowed only four-character passwords and never locked accounts when login attempts repeatedly failed. With these settings, user IDs are at risk of being compromised by attackers using brute-force password cracking software.
- At one of the Department's data centers, Rural Development manages 8,235 user IDs. Of those, 7,895 have passwords that are set to never expire despite Department and NIST guidelines that require the expiration of passwords. The data center has requested a waiver from Rural Development; however, Rural Development had not responded to this request.
- Our review of remote access accounts found that 782 could not be associated with a current employee or contractor. Of those, 723 did not have a user name associated with the account. Without a complete name to associate ownership, it is virtually impossible to determine who is using those accounts. Further, we found five former employees who still had active remote access accounts. One of those five, who has been deceased for over 3 years, was brought to Rural Development's attention in our 2001 audit.
- Our review of one of Rural Development's major applications found 16 user accounts with the ability to update production application programs. This access level was greater than those employees needed to perform their job functions. Of those, 8 did not need access to the application and the other 8 needed only read access. In another

major application that Rural Development uses to account for billions of dollars of loans, we identified three system developers that had the authority to update all transactions within that application's production database. Best practices dictate proper segregation of duties between system development and access to production databases to ensure the integrity of the system's data.

#### **Recommendation No. 5**

Establish a timeline to correct the systemic internal control weaknesses relating to logical access controls identified in this report.

**Agency Response.** This recommendation correlates with Recommendation Nos. 9 and 10 in OIG Report 85099-2-FM, Rural Development identified the actions planned to correct the systemic internal control weaknesses relating to logical access controls in our response to that report.

Rural Development will have a draft plan for the creation of verification reports with instructions to managers on the purpose and a full explanation of access privileges by March 2004. When these activities and certification and accreditation disaster recovery plan activities are completed, adequate controls will be in place.

**OIG Position.** We agree with Rural Development's actions to establish verification reports and provide instructions to managers. However, Rural Development's response did not address other access control weaknesses we identified such as establishing controls over remote access and inadequate system password settings. In order to reach management decision, Rural Development needs to provide us a response which addresses all the access control issues we identified and provide dates when those controls will be implemented.

---

#### **Finding 4**

#### **Rural Development is not Vigilant in Identifying and Correcting Identified System Vulnerabilities**

We again identified numerous vulnerabilities in Rural Development's systems, including some that remained despite Rural Development's knowledge of the vulnerabilities through its contractors in 1997, and reported by OIG in 1999 and again in 2001. Rural Development management has continually reported to us that it had taken actions to correct the previously



identified vulnerabilities. However, Rural Development had not taken adequate corrective actions to correct the vulnerabilities we identified, has not established controls to ensure all of its systems were scanned on a regular basis, or established effective controls to ensure that vulnerabilities identified by its own scans are timely corrected. As a result, Rural Development's systems are unnecessarily vulnerable to exploitation.

OMB Circular A-130 requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss. Further, the Department OCIO has established a policy<sup>24</sup> that agencies regularly scan their systems for known vulnerabilities using a Department-purchased vulnerability-scanning tool.

Our vulnerability assessments included 99 network components and disclosed 72 potentially high-risk,<sup>25</sup> and 143 potentially medium-risk vulnerabilities. Nearly half of the potentially high-risk vulnerabilities, which can give an attacker administrative access to a system, were accessible from outside of Rural Development's own network. This level of access would give an attacker complete control over a system. Examples of some of the high-risk vulnerabilities include:

- A software program was configured to use default settings, which included a blank administrator password. An unauthorized user who obtained access to that program and its administrator password could obtain administrative access to the entire system.
- A weakness in an older version of one system's operating software would allow a knowledgeable attacker to bypass authentication and gain full administrative privileges.
- A server was not adequately secured by allowing a default utility program to be accessible. This program would allow an attacker to view information on the server and possibly gain access to user IDs and passwords.

Our analysis of the 72 high-risk vulnerabilities identified 66 that could have been avoided had Rural Development timely patched its systems. Of those 66 vulnerabilities, 55 could have been corrected with a patch that had been available for over 1 year, and 9 others could have been corrected with a patch that had been available for over 5 years. We further found that Rural

---

<sup>24</sup> "Cyber Security Manual," DM 3500-2, Chapter 6, Part 1, dated April 4, 2003.

<sup>25</sup> High-risk vulnerabilities are those that provide access to the computer, and possibly the network of computers. Medium-risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher-risk vulnerabilities. Low-risk vulnerabilities are those that provide access to network data that might be sensitive, but less likely to lead to a higher-risk exploit.

Development had not maintained its virus protection software on all of its systems or patched its systems in a timely manner. Of the 23 security incidents<sup>26</sup> that occurred within Rural Development between June 2002 and June 2003, 4 were due to the virus software not being up to date, and 8 were caused because security patches had not been installed in a timely manner.

In its response to our prior audit report, Rural Development reported to us that it had corrected most of the vulnerabilities we identified. The remaining vulnerabilities, which required coordination with multiple commercial software vendors, were to be corrected and verified by June 2003. However, we identified vulnerabilities that simply required a password change that had still not been corrected. The vulnerabilities were passwords that matched the user ID, making it unnecessarily easy for an attacker to gain entry into these systems. These vulnerabilities were reported to Rural Development in our prior scans in 1999 and 2001, and were identified again by their own scans in 2003.

Rural Development also stated that they had formed an internal audit team to develop a proactive security plan including the running of a scanning tool on a periodic basis to determine that systems are updated with the latest patches and service packs. We found that this team had since been assigned to other projects and was not performing vulnerability scans, consequently not all of its servers had been scanned on a monthly basis as required by the Department and its own policy.<sup>27</sup> It is apparent that Rural Development has not addressed the systemic weaknesses in its internal controls and simply reacted to the findings in our report.

Finally, Rural Development instituted a server checklist in response to our prior audit to ensure compliance with agency and Department policies, and as an oversight tool for security staff to monitor system administration functions. This checklist included documentation of system location, operating system and applications, system owner, and key personnel. While Rural Development considered this a major accomplishment in its June 2003 POA&M, we found that the checklist was not completed with all of the information needed to serve as a useful tool for the security staff. For instance, some of the basic information such as the operating system was left blank for 358 out of the 478 servers. In addition, only 9 of the 478 servers showed that Rural Development had scanned those systems using its vulnerability scanning software.

---

<sup>26</sup> Rural Development lack of adequate security incident response report under Finding No. 2.

<sup>27</sup> Rural Development "Server Policy," dated April 2001.

## Recommendation No. 6

Establish controls, including second party review and oversight, to ensure that vulnerability scans are performed timely and accurately, and that corrective action on the vulnerabilities identified are immediately resolved.

**Agency Response.** The OCIO-CS runs scans on Rural Development systems on a continuous basis. The Information Technology Working Group Inter-Operability Laboratory runs scans of field office systems for specific vulnerabilities on a continuous basis.

Rural Development will take corrective actions to correct the vulnerabilities identified by OIG and will establish controls to ensure that vulnerabilities identified by its own scans are timely corrected.

Rural Development runs scans on the web farm, Washington, D.C. systems, St. Louis systems, and on systems for one-third of the country based on a memorandum of understanding with ITWG. Web farm, St. Louis, and ITWG scan results are tracked on a spreadsheet until the actions are closed. Washington, D.C. scan results are discussed in weekly meetings, and a tracking mechanism will be developed.

**OIG Position.** We agree with Rural Development's proposed actions; however, Rural Development needs to describe the specific controls it intends to implement to ensure that vulnerability scans are accurately conducted and that identified vulnerabilities are timely corrected.

## Recommendation No. 7

Establish controls to ensure timely application of system updates and patches, and that virus software is installed and systematically updated.

**Agency Response.** Rural Development uses PatchLink, a software utility that provides enterprise-wide software distribution capabilities, in the web farm and is in the process of implementing it in St. Louis and Washington, D.C. to verify that all patches have been applied to the systems.

PatchLink has two components: PatchLink Update Server and agent software. The agent will be installed on all St. Louis Rural Development workstations. A deployment plan has been developed for the St. Louis Rural Development organizations at all three sites. The deployment will be accomplished in phases beginning on February 11, 2004 with specific subnets identified in each phase.

**OIG Position.** We agree that Rural Development's implementation of Patchlink software will improve its abilities to ensure software and operating

system patches are timely deployed; however, Rural Development needs to establish policies on the use of Patchlink and controls to ensure the effective use of the product in its environment (i.e., testing patches in a test environment before deployment). In order to reach management decision, Rural Development needs to provide a date when Patchlink will be installed and implemented on all agency systems, and establish controls over the patch management process.

### Section 3. Application Change Controls

---

#### Finding 5. Application Change Controls Need Strengthening

Rural Development was not following its own policies<sup>28</sup> for identifying, selecting, installing, and modifying software. Further, those policies did not conform to departmental, NIST, and OMB guidance regarding change controls and segregation of duties. Hence, we were unable to validate that system software changes (1) received proper authorization, (2) were supported by change request documents, (3) were properly tested and test results approved, or (4) were properly monitored while being moved into production environment. Rural Development officials were unable to provide us a plausible explanation for this internal control weakness, but agreed that they needed to conform to proper change control procedures. Without proper software change controls, Rural Development cannot be assured that:

- System functions are performing as intended;
- data residing on, and extracted from, the system is reliable;
- only authorized and tested changes are made;
- malicious programs are not introduced into the system; and
- security features are not inadvertently or deliberately omitted or rendered inoperable.

USDA DM 3200-2.2<sup>29</sup> requires a change control process for all major application systems, which properly documents the change process including approval and acceptance of changes and testing the changes in a system test environment. The manual states that, "the process may include a change control board or an individual who is responsible for ensuring that all changes have been properly evaluated."

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook," 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,<sup>30</sup> "Guide for the Security Certification and Accreditation

---

<sup>28</sup> "Rural Development Application Information Systems Support Handbook," dated May 1997.

<sup>29</sup> DM 3200-2.2, "A Project Manager's Guide to Application Systems Life Cycle Management," Section 1.3.B (7)(a), (b), and (d), dated March 3, 1988.

<sup>30</sup> NIST SP 800-37, dated June 30, 2003, is still in draft and will replace Federal Information Processing Standards Publication (FIPS) 102, "Guidelines for Computer Security Certification and Accreditation," dated September 27, 1983, which is still current, FIPS 102 discusses these issues on page 19, Section 1.5.2; page 52, Section 2.7; and page 54, Section 2.7.3.

of Federal Information Systems,” it is important to document the 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 A-130<sup>31</sup> 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.”

Our review of 20<sup>32</sup> completed application changes disclosed that system changes were not properly authorized or approved before changes were implemented. The following describes some of the system change weaknesses identified.

- Of the 20 system changes, 14 did not have test plans and test results to demonstrate that changes were tested and approved before being placed into the production environment.
- System changes in two instances were requested and approved by the same person, which is a separation of duties issue.
- Controls were not in place over changes made by system programmers to the production environment. We identified occurrences where system programmers were making changes directly in the production libraries without first being authorized and changes were being made outside the change management software so no audit trail was being created. This is further complicated by the fact that we identified 16 system users who had been given update authority to the production libraries even though their job functions did not require this access. (See Finding No. 3.)
- System change requests were inconsistently documented and did not contain all required details to authorize and implement the system change.
- Emergency changes are not subject to the same review, testing, and approval process that apply to scheduled changes. Because Rural Development does not have a process to identify emergency changes in its change request log, no followup and approval was completed after implementation of the emergency change.

---

<sup>31</sup> OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources,” dated November 30, 2000.

<sup>32</sup> To review Rural Development’s Life Cycle Management process, OIG randomly selected a sample of 20 Requests For Automation from a total of 135 modifications made between April 1, 2002, through April 1, 2003, to one of its major applications.

Additionally, we determined that Rural Development was not effectively and efficiently using its mainframe change management software to control production software changes. Rural Development did not always use its change management software to move a system change into the production libraries. Instead, we found instances where changes were being made directly in the production libraries without being properly authorized or approved. This practice created numerous problems for the change management group when they subsequently tried to implement changes through the change management software. Because the production source code did not match the executable program load modules maintained by the change control software, programmers had to keep fixing the same problem over and over again because the problem kept reappearing.

Finally, Rural Development uses change management software that allows it to move applications from the development environment into the production environment. The software has the capability to compare the program in each environment to ensure the program running in production is the approved program. However, Rural Development did not use the change management software to ensure that the approved application programs matched the actual application program being executed in the production environment. Rural Development officials were not aware of this feature; consequently, it had not been implemented. As a result, Rural Development cannot be assured that it is running the latest, approved programs and that changes are being properly monitored and properly protected.

### **Recommendation No. 8**

Establish controls to ensure that change control procedures include documenting authorizations and testing before changes are implemented.

**Agency Response.** While Rural Development does have in place controls that, for the most part, ensure that change control procedures include documenting authorizations and testing before changes to mainframe applications are implemented, these controls can be enhanced.

Rural Development will conduct a comprehensive review of the change control process for all major applications and the general support system. The review will include ensuring that Agency policies are in compliance with Departmental, NIST and OMB guidance regarding change control and segregation of duties.

Based on this review, appropriate changes will be made to agency policies and mechanisms will be put in place to ensure adherence to the policies. Milestones and timeframes will be provided when the review is initiated.

**OIG Position.** In order to reach management decision, Rural Development needs to provide a date when their comprehensive review of the change control process will be performed.

### **Recommendation No. 9**

Establish controls to ensure that all changes are properly recorded and that records contain all relevant information on the change.

**Agency Response.** While Rural Development does have in place controls that, for the most part, ensure that all changes to mainframe applications are properly recorded and that records contain all relevant information on the change, these controls can be enhanced.

Rural Development will conduct a comprehensive review of the change control process for all major applications and the general support system. The review will include ensuring that Agency policies are in compliance with Departmental, NIST and OMB guidance regarding change control and segregation of duties.

Based on this review, appropriate changes will be made to agency policies and mechanisms will be put in place to ensure adherence to the policies. Milestones and timeframes will be provided when the review is initiated.

**OIG Position.** In order to reach management decision, Rural Development needs to provide a date when their comprehensive review of the change control process will be performed.

### **Recommendation No. 10**

Establish controls to prevent the change control software from being circumvented.

**Agency Response.** Rural Development has taken immediate action to remove update authority for 13 of the 16 users who were identified as having update authority even though their job functions did not require this access. The other three users are the system developers who were identified as having the authority to update all transactions within one of our major application's production database. Update authority has been removed for one of these users. The other two users require update authority under limited circumstances to assure the continued operation of the application. Control of the update authority for these users will be temporarily assigned to the change control manager pending the outcome of the comprehensive review described below.



Rural Development will conduct a comprehensive review of the change control process for all major applications and the general support system. The review will include ensuring that Agency policies are in compliance with Departmental, NIST and OMB guidance regarding change control and segregation of duties.

Based on this review, appropriate changes will be made to agency policies and mechanisms will be put in place to ensure adherence to the policies. Milestones and timeframes will be provided when the review is initiated.

**OIG Position.** While we agree with Rural Development's decision to remove update access for several users, additional actions are needed to ensure the integrity of the application change control process. In order to reach management decision, Rural Development needs to fully explain the controls it intends to establish over update authority, and provide us a date when it will complete its review of its change control process.

**Finding 6**

**IT Controls at State and County Offices Need Strengthening**

Rural Development has not ensured that all IT security controls are in place at its State and county offices. Specifically, State and county offices had not adequately maintained contingency planning documents, physically secured IT equipment, and ensured that all of its field employees received security awareness training. While Rural Development had IT policies in place, it had no controls established to enforce those policies at the State and county levels. As a result, Rural Development cannot be assured that its IT resources are properly secured at its remote offices.

OMB Circular A-130 requires that agencies prepare contingency plans and that those plans be periodically tested. OMB also requires that agencies establish adequate controls to ensure that IT assets are adequately protected, and that employees receive training to ensure they are aware of their security responsibilities. Further, DR 3140-1 and Rural Development's security handbook require annual security awareness training for all employees.

Contingency Planning

Of the 10 State and county offices we visited, only 1 had an adequate contingency plan. Of the remaining nine offices, two could not locate their contingency plans and seven had plans that lacked sufficient detail to ensure a successful recovery in the event of an actual emergency. For example, one contingency plan's 'notification' section contained the names of nine personnel that were no longer employed by Rural Development, and its 'Off-site Storage Location' section was left blank.

A critical component of any contingency plan is the planning for data backups and the storage of backup media. We found that backup procedures were being performed at all locations we visited where that responsibility was assigned to Rural Development;<sup>33</sup> however, six offices did not adequately store their backup tapes to prevent their destruction in the event of a disaster. For example, one office was storing the backup tapes in the same room as the system. In order to ensure the safety and reliability of backup tapes during an emergency, backup tapes should be stored a safe distance from the main operating environment.

---

<sup>33</sup> The responsibility for backups was assigned to another CCE agency at one of the offices visited.

### Physical Access Controls

Physical access controls restrict access to computer resources to only those personnel who need access to administer the systems and ensure that the data that reside on those systems is not compromised. At 5 of the 10 State and county offices we visited, we observed that critical systems were left in common areas or unsecured supply closets to which everyone had access. For example, at one office the server was located in a storage room. This storage room was the only path that leads to the employee break room. Therefore, employees moved back and forth through this room throughout the day. At another location, the server room was left unlocked throughout the day. While the server room door was secure in the evenings, the room had an unsecured exterior window that would allow easy access to anyone.

### Security Awareness Training

Of the 10 offices we visited, employees at 9 of those offices had not received their annual security awareness training. While some training had been initiated in five of the nine offices, security awareness training had not taken place in over 2 years in the remaining four offices. Rural Development has issued a comprehensive security handbook that outlines policy, assigns responsibility, and identifies controls that are to be implemented to protect Rural Development information. The handbook is specifically designed for individual employee users and is a great supplement to the annual security awareness training. However, while the handbook contains comprehensive information to ensure good security practices when implemented, the handbook becomes ineffective unless employees have access to it. We found that employees in 6 of the 10 offices we visited did not have a copy of the security handbook. Without providing employees with adequate annual security training or access to comprehensive security guidance, Rural Development cannot ensure employees understand or be held accountable for basic security responsibilities.

### **Recommendation No. 11**

Establish controls that Rural Development's policies are implemented at the local office level.

**Agency Response.** ITWG is developing a user and technical security policy for use at the local office level. Rural Development is represented on the ITWG group. The ISSPM review is scheduled for the third quarter of Fiscal Year 2004. Subsequent to the ISSPM review, the manual will be distributed to the ITWG team leaders for general review.

Rural Development also conducts State Internal Reviews to ensure that IT security controls are in place at the State and County Office level. The review is conducted using the State Internal Review Handbook which includes an Information Resources Management Review Guide.

Rural Development also has an Administrative Review process in place that includes a review of IT security policies at the local office level. Rural Development offices in Mississippi were reviewed in June 2003.

**OIG Position.** We agree with Rural Development's proposed actions; however, our review indicated that, while policies existed, Rural Development did not have controls in place that ensured the effective implementation of the established policies. In order to reach management decision, Rural Development needs to provide assurance that the user and technical security manual being prepared by the Information Technology Working Group will cover the issues identified in our report, and that Rural Development-initiated State and county office reviews be strengthened to ensure the enforcement of those policies. Finally, Rural Development needs to provide dates when both of these actions will be implemented.

## ***Scope and Methodology***

---

The audit was conducted in accordance with Government Auditing Standards from May through October 2003.

We tested selected Rural Development computer networks to identify vulnerabilities that could enable unauthorized users to access sensitive data stored on or transmitted over Rural Development systems. We used commercially available software applications to assist us in our security review of Rural Development network components located in St. Louis, Missouri, and Washington, D.C. Network components were judgmentally selected for review from Rural Development's list of components and our discovery scans. The universe of Rural Development network components could not be determined because Rural Development's network spans numerous office locations in Washington, D.C., St. Louis, Missouri, 47 States and county-based service centers.

We also performed limited scope testing at judgmentally selected State and county Rural Development offices, based on program activity, to evaluate the adequacy of IT controls in those offices. A total of 10 State and county offices were visited in the states of Alabama, Minnesota, Iowa, Oregon, and Pennsylvania.

## **General Comments**

---

The weaknesses disclosed in this report represent, in our opinion, material internal control weaknesses in Rural Development's ability to secure its IT resources, including those resources that impact its financial management and reporting functions. Therefore, Rural Development needs to identify these material weaknesses in its FMFIA report until corrected.

# Exhibit A – History of OIG Evaluations of Rural Development IT Controls

ISSUE <sup>34</sup>	EVALUATIONS									
	FmHA <sup>35</sup> Debt and Loan Restructuring System, November 1988 (04673-3-SF)	Audit of National Systems Application Programs Standards for Testing, January 1990 (04099-70-FM)	FmHA Controls and Security Over Remote Transaction Processing, February 1992 (04600-4-FM)	National Standards and Technology Evaluation of FmHA Information Systems Security Program, July 1992	FmHA Selected Aspects of FmHA Computer Security, March 1994 (04099-89-FM)	UNISYS Rural Development Network Risk Analysis, March 1997	Audit of the Rural Development Consolidated Financial Statements for Fiscal Year 1997, May 1998 (50401-21-FM)	Rural Development's Information System Controls Need Strengthening, March 2000 (85099-01-FM)	Security Over Rural Development's Information Technology Resources Needs Improvement, August 2002 (85099-02-FM)	Review of Rural Development's Information Technology Resources Security (85099-04-FM--This report.)
1. System Testing / Certification	X	X		X	X		X		X	X
2. Testing of Applications / Control over Production Libraries	X	X		X	X	X	X			X
3. Security Program			X	X	X	X	X	X	X	X
4. Access Controls			X		X	X	X	X	X	X
5. Disaster Recovery / Contingency Plan					X	X	X			X
6. Secure Access to Internet						X	X	X	X	X
7. Remote Access			X			X		X	X	X
8. Passwords					X	X		X	X	X
9. Physical Security						X	X			X
10. Organizational Structure		X							X	X
11. Training								X	X	X
12. Incident Response Procedures								X	X	X

<sup>34</sup> The scope of each evaluation did not include all issues.

<sup>35</sup> The USDA underwent a major reorganization and realignment of program areas involving the activities of the farm, rural housing, and rural development programs managed by Farmer's Home Administration (FmHA) and Rural Development Administration (RDA). During USDA's reorganization in October 1994, the loan and grant programs managed by FmHA and RDA were combined with other programs in the newly created Rural Development agency.



United States  
Department of  
Agriculture

Rural Development

Operations and  
Management

Washington, DC  
20250

REPLY TO  
ATTN OF: FC-421

SUBJECT: Office of Inspector General Report 85099-4-FM

TO: John Purcell  
Director, Financial Management Division

THROUGH: Sherie Hinton Henry *Sherie Hinton Henry 2/17/04*  
Deputy Administrator for  
Operations and Management

FROM: *for* Thomas E. Hannah *TEH*  
Chief Information Office

As requested in your memorandum dated January 16, 2004, following is information related to the recommendations in Office of Inspector General (OIG) Report 85099-4-FM, Review of Rural Development's Information Technology Resources Security.

As was discussed during the exit conference held on January 6, 2004, some recommendations in this report are very similar to recommendations in OIG Report 85099-2-FM, Security Over Rural Development's Information Technology Resources Needs Improvement. Consequently, some actions taken to resolve the findings will overlap between the two reports.

Recommendation 1

Until funding is obtained to implement broader organizational changes, implement interim measures with specific timeframes for achievement to ensure that security controls, including those recommended elsewhere in this report, are implemented and effectively carried out.

Comments

This recommendation correlates with Recommendation 1 in OIG Report 85099-2-FM. In OIG's response to Recommendation 1, while acknowledging that Rural Development does not have authority to realign the Information Technology Staff until the Common Computing Environment

Rural Development is an Equal Opportunity Lender. Complaints of discrimination should be sent to: Secretary of Agriculture, Washington, DC 20250





2

convergence is complete, OIG states that Recommendation 1 will remain outstanding until Rural Development, along with the Office of the Chief Information Officer (OCFO), can agree to and implement an effective management structure over Rural Development's information security program.

The Deputy Administrator for Operations and Management (DAOM) is shown organizationally under the Administrator, Rural Housing Service, for budgetary purposes only. For all other purposes, the DAOM reports directly to the Under Secretary for Rural Development. Accordingly, the Under Secretary is the second level of command for the Chief Information Officer (CIO).

The Rural Development CIO is assigned to a higher level within the organizational structure than the CIO in the Service Center partner agencies. For example, in the Farm Service Agency, the Under Secretary is the third level of command for the CIO.

Rural Development has taken steps to ensure that security controls, including those recommended elsewhere in this report, are implemented and effectively carried out.

Effective January 12, 2004, the Information Systems Security Staff (ISSS) was reassigned to report directly to the Deputy Chief Information Officer (DCIO). This emphasizes the level of importance current management places on security issues and frees the security staff from the normal internal debates on prioritization by establishing security as always having the highest CIO priority and allows the ISSS to effectively implement the Agency's Information Systems Security Program (ISSP).

In addition, an onsite security position was established in the Washington, D.C., office as the liaison with ISSS on Washington, D.C., related security issues. Responsibilities of this position include coordinating and reviewing general support system or major application risk assessments, security plans, and mitigation efforts; assisting in identifying, researching, mitigating, and reporting on security-related information pertaining to incidents and acknowledged or suspected weaknesses and vulnerabilities in the agency's information systems; and assisting in gathering, resolving, and reporting on Departmental, oversight agency, and agency internal and external audit information and mitigation efforts.

3

Weekly meetings were initiated in December 2003 between the Washington, D.C., liaison and the ISSS to discuss open security related issues. A tracking spreadsheet has been created which includes the issue, the date it was raised, the responsible entity, and the status. This has greatly improved the standardization of security throughout Rural Development and provides a means of communication of issues from both perspectives, the Washington, D.C., community and ISSS.

To further ensure that security controls are implemented and effectively carried out, a project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the Information Systems Security Program Manager (ISSPM) and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

The team also plans to have periodic discussions, possibly on a monthly basis, with OIG staff to clarify issues and to assist in ensuring that proposed corrective actions address the systemic cause of the audit findings.

#### Recommendation 2

Rural Development needs to establish a second-party review within its management decision process relating to Information Technology to ensure that the corrective actions proposed address the systemic cause of the audit finding. Further, follow-up needs to be done at the National office level to ensure corrective actions have been effectively implemented before final action is forwarded to the OCFO.

#### Comments

The Rural Development audit resolution and review process starts with subject matter experts and evolves through the various levels of management. The subject matter experts, for example the ISSS for security findings, provide detail information that is included in the project plan and is the source of the response to OIG to reach management decision and to the OCFO to support requests for final action. The information gathered from the subject matter experts, in addition to research of other sources, is used by the Financial Management Systems Branch representatives to formulate the responses.

4

Once formulated, the proposed corrective actions are reviewed by the subject matter experts, the DCIO, the CIO, and the DAOM prior to submission to OIG and/or to QCFO.

A project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the Information Systems Security Program Manager (ISSPM) and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

The team also plans to have periodic discussions, possibly on a monthly basis, with OIG staff to clarify issues and to assist in ensuring that proposed corrective actions address the systemic cause of the audit findings.

#### Recommendation 3

Establish a plan of action with specific timeframes and allocate appropriate resources to establish policies and controls to ensure compliance with Office of Management and Budget (OMB) Circular A-130 and FISMA.

#### Comments

This recommendation correlates with Recommendation 2a in OIG Report 50401-21-FM, Audit of the Rural Development Consolidated Financial Statements for Fiscal Year 1997. We request that Recommendation 2a be closed and that future activities related to OMB Circular A-130 be addressed under Recommendation 3 in the subject report.

Rural Development is in the midst of certification and accreditation of its major applications and general support system in accordance with OMB Circular A-130. Security certification is a comprehensive assessment of a system's technical and non-technical security features and safeguards which establishes whether the system and its operating environment meet a set of specified security requirements and provides a comprehensive factual basis for making an accreditation decision. System accreditation is a management decision by senior agency official(s) authorizing operation of Information Technology systems based upon the

5

certification process as documented in a certification package and explicitly defines and accepts residual risks present in the subject systems. Information Technology contingency planning is included in the certification and accreditation process.

Certification and accreditation activities performed during the first quarter of Fiscal Year 2004 were primarily preparatory and planning oriented. Tools were created and refined for guiding and streamlining certification and accreditation efforts including templates for performing privacy impact assessments, secure features users guides, and trusted facilities manuals.

An important focus of the early stage of certification and accreditation activities was to establish good communications with the United States Department of Agriculture key players who will be integral to the whole certification and accreditation activities effort. This was accomplished through meetings, slide presentations, and the creation and distribution of certification and accreditation activities tool kits to the system owners.

Rural Development would like to meet with OIG to discuss requirements for closing this recommendation to ensure that we have a mutual understanding of the specific steps that need to be addressed. The finding and recommendation in OIG Report 85099-2-FM, as well as in this report, are very broad. Rural Development believes that by concentrating on certification and accreditation, disaster recovery plan, and Federal Information Security Management Act (FISMA) compliance while addressing access control and other outstanding audit issues, we will have come a long way to bringing our ISSP into compliance with OMB Circular A-130. We would like to specifically identify any other steps that are required for OIG to consider this item closed.

#### Recommendation 4

Establish controls over the Plan of Action and Milestones (POAM) reporting process, including a second party review, to ensure that weaknesses are properly reported and that milestones reflect effective and measurable actions toward completion of the weakness.

6

#### Comments

The Rural Development POAM is the official document for reporting to the Office of the Chief Information Officer-Cyber Security (OCIO-CS) on actions being taken to improve and strengthen the Rural Development Information System Security Program (ISSP) and the individual major applications and general support system in conformance with Federal and Departmental requirements.

The POAM update was reformatted to conform to recently released Office of Management and Budget/OCIO-CS guidelines regarding the FISMA and the weaknesses and vulnerabilities identified during the analyses of the Fiscal Year 2003 FISMA submission. Existing and newly defined milestones will be integrated into appropriate POAM's for the overall ISSP and each major application and general support system.

To further ensure that security controls are implemented and effectively carried out, a project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the ISSPM and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

Audit resolution information from the project plan is included in the POAM. Quarterly status reports, including an executive summary, are submitted to the OCIO-CS. Prior to submission to the OCIO-CS, the executive summary is reviewed and approved by the DCIO, the CIO, and the DAOM. The Rural Development program administrators are provided copies of the quarterly POAM status reports. OCIO-CS reviews, scores, and consolidates the detail information into a Departmental report.

#### Recommendation 5

Establish a timeline to correct the systemic internal control weaknesses relating to logical access controls identified in this report.

7

**Comments**

This recommendation correlates with Recommendations 9 and 10 in OIG Report 85099-2-FM. Rural Development identified the actions planned to correct the systemic internal control weaknesses relating to logical access controls in OIG Report 85099-2-FM.

Rural Development will have a draft plan for the creation of verification reports with instructions to managers on the purpose and a full explanation of access privileges by March 2004. When these activities and certification and accreditation disaster recovery plan activities are completed, adequate access controls will be in place.

To further ensure that security controls are implemented and effectively carried out, a project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the Information Systems Security Program Manager and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

**Recommendation 6**

Establish controls, including second party review and oversight, to ensure that vulnerability scans are performed timely and accurately, and that corrective action on the vulnerabilities identified are immediately resolved.

**Comments**

The OCIO-CS runs scans on Rural Development systems on a continuous basis. The Information Technology Working Group Inter-Operability Laboratory runs scans on field office systems for specific vulnerabilities on a continuous basis.

Rural Development will take corrective actions to correct the vulnerabilities identified by OIG and will establish controls to ensure that vulnerabilities identified by its own scans are timely corrected.

8

Rural Development uses PatchLink, a software utility that provides enterprise-wide software distribution capabilities, in the web farm and is in the process of implementing it in St. Louis and Washington, D.C., to verify that all patches have been applied to the systems. Unapplied patches are installed and exceptions are tracked on a spreadsheet.

Rural Development runs scans on the web farm, Washington, D.C., systems, St. Louis systems, and on systems for one-third of the country based on a memorandum of understanding with ITWG. Web farm, St. Louis, and ITWG scan results are tracked on a spreadsheet until the actions are closed. Washington, D.C., scan results are discussed in weekly meetings and a tracking mechanism will be developed.

The Alert Team distributes notification of vulnerabilities and patches to system administrators in the web farm, St. Louis, and Washington, D.C., and tracks followup activities in a tracking data base.

Rural Development will implement PatchLink across our network. This capability is especially needed in order to apply critical security patches in a timely manner. It also provides monitoring and reporting capabilities to track the status of the patch updates.

PatchLink has two components: PatchLink Update Server and agent software. The agent will be installed on all St. Louis Rural Development workstations. A deployment plan has been developed for the St. Louis Rural Development organizations at all three sites: 4300 Goodfellow Boulevard, 1520 Market Street, and 2350 Market Street. The deployment will be accomplished in phases beginning on February 11, 2004, with specific subnets identified in each phase.

During the initial deployment process, PatchLink will perform a discovery of the workstations assigned to the subnets and register them to its server; will push the client PatchLink agent to all the workstations in the subnets; and will deploy the recently released Microsoft patch (Microsoft Security Bulletin MS04-004).

#### Recommendation 7

Establish controls to ensure timely application of system updates and patches, and that virus software is installed and systematically updated.

9

#### Comments

OCIO-CS runs scans on Rural Development systems on a continuous basis. The Information Technology Working Group Inter-Operability Laboratory runs scans on field office systems for specific vulnerabilities on a continuous basis.

Rural Development will take corrective actions to correct the vulnerabilities identified by OIG and will establish controls to ensure that vulnerabilities identified by its own scans are timely corrected.

Rural Development uses PatchLink, a software utility that provides enterprise-wide software distribution capabilities, in the web farm and is in the process of implementing it in St. Louis and Washington, D.C., to verify that all patches have been applied to the systems. Unapplied patches are installed and exceptions are tracked on a spreadsheet.

Rural Development runs scans on the web farm, Washington, D.C., systems, St. Louis systems, and on systems for one-third of the country based on a memorandum of understanding with ITWG. Web farm, St. Louis, and ITWG scan results are tracked on a spreadsheet until the actions are closed. Washington, D.C., scan results are discussed in weekly meetings.

The Alert Team distributes notification of vulnerabilities and patches to system administrators in the web farm, St. Louis, and Washington, D.C., and tracks followup activities in a tracking data base.

Rural Development will implement PatchLink across our network. This capability is especially needed in order to apply critical security patches in a timely manner. It also provides monitoring and reporting capabilities to track the status of the patch updates.

PatchLink has two components: PatchLink Update Server and agent software. The agent will be installed on all St. Louis Rural Development workstations. A deployment plan has been developed for the St. Louis Rural Development organizations at all three sites: 4300 Goodfellow Boulevard, 1520 Market Street, and 2350 Market Street. The deployment will be accomplished in phases beginning on February 11, 2004, with specific subnets identified in each phase.

During the initial deployment process, PatchLink will perform a discovery of the workstations assigned to the subnets and register them to its server; will push the client PatchLink agent to all the workstations in the subnets; and will deploy the recently released Microsoft patch (Microsoft Security Bulletin MS04-004).



10

Recommendation 8

Establish controls to ensure that change control procedures include documenting authorizations and testing before changes are implemented.

Comments

Rural Development does have in place controls that, for the most part, ensure that change control procedures include documenting authorizations and testing before changes to mainframe applications are implemented. In accordance with United States Department of Agriculture Departmental Manual (DM) 3200-2.2, A Project Manager's Guide to Application Systems Life Cycle Management, our process includes a change control group that is responsible for ensuring that all changes have been properly evaluated. This group reviews all change packages before including them in releases to the production library. The package must include a reference to the request for automation or problem report that authorizes the change and other documentation, including user acceptance letters. In these letters, user representatives certify that they approve changes made for the request, that the results of the test output are acceptable, and that the change should be moved into production. The change control group will not accept any packages that do not include user acceptance letters.

We do recognize that these controls can be enhanced.

Rural Development will conduct a comprehensive review of the change control process for all major applications and the general support system. The review will include ensuring that Agency policies are in compliance with Departmental, National Institute of Standards and Technology (NIST), and OMB guidance regarding change control and segregation of duties.

Based on this review, appropriate changes will be made to agency policies and mechanisms will be put in place to ensure adherence to the policies. Milestones and timeframes will be provided when the review is initiated.

To ensure that security controls are implemented and effectively carried out, a project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the Information Systems Security Program Manager and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual

11

responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

Recommendation 9

Establish controls to ensure that all changes are properly recorded and that records contain all relevant information on the change.

Comments

Rural Development does have in place controls that, for the most part, ensure that all changes to mainframe applications are properly recorded and that records contain all relevant information on the change. Each change must be supported by a request for automation or a problem report. The requests for automation and problem reports are submitted to the appropriate Information Resources Management organization to be recorded in the Request for Automation Tracking System. If the request for automation or problem report does not include all relevant information on the change to be properly evaluated, it is returned to the submitter for additional information.

We do recognize that these controls can be enhanced.

Rural Development will conduct a comprehensive review of the change control process for all major applications and the general support system. The review will include ensuring that Agency policies are in compliance with Departmental, NIST, and OMB guidance regarding change control and segregation of duties.

Based on this review, appropriate changes will be made to agency policies and mechanisms will be put in place to ensure adherence to the policies. Milestones and timeframes will be provided when the review is initiated.

To ensure that security controls are implemented and effectively carried out, a project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the Information Systems Security Program Manager and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

12

Recommendation 10

Establish controls to prevent the change control software from being circumvented.

Comments

Rural Development has taken immediate action to remove update authority for 13 of the 16 users who were identified as having update authority even though their job functions did not require this access. We note there is no evidence that these users inappropriately used that authority to make changes directly in the production libraries without first being authorized. The other three users are the system developers who were identified as having the authority to update all transactions within one of our major application's production data base. Update authority has been removed for one of these users. The other two users require update authority under limited circumstances to assure the continued operation of the application. Control of the update authority for these users will be temporarily assigned to the change control manager pending the outcome of the comprehensive review described below.

Rural Development will conduct a comprehensive review of the change control process for all major applications and the general support system. The review will include ensuring that Agency policies are in compliance with Departmental, NIST, and OMB guidance regarding change control and segregation of duties.

Based on this review, appropriate changes will be made to agency policies and mechanisms will be put in place to ensure adherence to the policies. Milestones and timeframes will be provided when the review is initiated.

To ensure that security controls are implemented and effectively carried out, a project plan has been put in place to monitor and track all outstanding audit findings, with particular emphasis on those related to the security program. The project plan is maintained on a spreadsheet and is monitored by a team which includes the Information Systems Security Program Manager and representatives from the Financial Management Systems Branch. Weekly team meetings are held to determine corrective actions needed, to establish timeframes and individual responsibility for corrective actions, and to review the status of proposed corrective actions. The project plan is a living document that is submitted to the DCIO on a bi-weekly basis. Oversight is provided by the DCIO and the CIO.

13

Recommendation 11

Establish controls that Rural Development's policies are implemented at the local office level.

Comments

ITWG is developing a user and technical security policy for use at the local office level. Rural Development is represented on the ITWG group. The ISSPM review is scheduled for the third quarter of Fiscal Year 2004. Subsequent to the ISSPM review, the manual will be distributed to the ITWG team leaders for general review.

Annual security awareness training is mandated by the Computer Security Act of 1987, the Federal Information Security Management Act of 2002, OMB Circular A-130, United States Department of Agriculture Departmental Regulation 3140-1, and the Rural Development Employee Security Handbook. Each year the agency is required to provide training to all employees, volunteers, contractors, or others who have access to agency computer systems.

In response, the United States Department of Agriculture, together with the Office of Personnel Management, and other federal agencies, developed online computer security awareness training using Goleam. This online training is designed to be taken by all of the United States Department of Agriculture employees to ensure consistency of the training across the United States Department of Agriculture and provide accountability for the training. The Department set aside the month of September 2003 for completion of security awareness training by all the United States Department of Agriculture employees.

Course completion information was provided to the agency ISSS for reporting and tracking purposes. This information was shared with managers to ensure that all contractors, volunteers, and employees complete the appropriate courses within the designated timeframes.

Rural Development also conducts State Internal Reviews (SIR) to ensure that Information Technology security controls are in place at the State and County Office level. SIR's consist of a comprehensive evaluation by State managers of the delivery of programs and administrative functions within the State.

14

The SIR process is a State management review of operations in field offices and centralized program functions to determine if policies and procedures for making and servicing loans/grants are being implemented according to Rural Development regulations and policy; determine if policies and procedures for working with supported and targeted communities are being implemented as directed; evaluate the effectiveness of administrative operations, including but not limited to, personnel management, contracting, collections and disbursements, civil rights monitoring, and automated systems; identify weaknesses or deficiencies in the program and administrative operations with specific corrective actions for their elimination or reduction and timeframes for completion; recognize effective field office and centralized program function activities in the delivery of program and in the management of personnel and resources; assess the effectiveness of management controls to minimize the potential for fraud, waste, unauthorized use, or mismanagement in office operations; inform the State Director of the status of operations; inform the State Director of the status of operations and controls in all offices; and inform the Rural Development Deputy Under Secretary for Operations and Management and Agency Administrators of the effectiveness of the State's oversight responsibilities.

The review is conducted using the State Internal Review Handbook which includes an Information Resources Management (IRM) Review Guide. The IRM Review Guide focuses primarily on security issues.

Rural Development also has an Administrative Review process in place that includes a review of Information Technology Security policies at the local office level. Rural Development offices in Mississippi were reviewed in June 2003.

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

Informational copies of this report have been distributed to:

Agency Liaison Officer  
General Accounting Office  
Office of Management and Budget  
Office of the Chief Financial Officer  
Director, Planning and Accountability Division