



U.S. Department of Agriculture

---



Office of Inspector General  
Great Plains Region

# **Audit Report**

## **Risk Management Agency Management and Security of Information Technology Resources**

Report No. 05099-18-KC  
June 2004

---



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



DATE: June 1, 2004

REPLY TO  
ATTN OF: 05099-18-KC

SUBJECT: Risk Management Agency Management and Security of Information Technology Resources

TO: Ross J. Davidson, Jr.  
Administrator  
Risk Management Agency

ATTN: Michael Hand  
Deputy Administrator  
for Compliance

This report presents the results of our review of Management and Security of Information Technology Resources. Your April 14, 2004, written response to the official draft report is included as exhibit B with excerpts and the Office of Inspector General's (OIG) position incorporated into the Findings and Recommendations section of the report.

Your response indicated that the Risk Management Agency conditionally concurs with many recommendations and included evidence that the agency has initiated partial corrective action on some recommendations. We were able to accept management decision on Recommendation No. 19. Please follow your agency's internal procedures in forwarding documentation for final action to the Office of the Chief Financial Officer. For the remaining recommendations, we were unable to accept management decision because the response did not include estimated timeframes for completion of corrective actions and/or detailed information on other key components of the recommendations. The additional information and/or actions needed are outlined in the report sections OIG Position.

Please furnish a reply within 60 days describing corrective actions taken or planned and the timeframes for implementing the corrective action on the recommendations where management decisions have not been reached. Please note that Departmental Regulation 1720-1 requires a management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance, and final action should be completed within 1 year of management decision.

We appreciate the courtesies and cooperation extended to our staff during the review.

/s/

ROBERT W. YOUNG  
Assistant Inspector General  
for Audit

# **Executive Summary**

## **Risk Management Agency Management and Security of Information Technology Resources (Audit Report No. 05099-18-KC)**

---

### **Results in Brief**

This report presents the results of our audit of Management and Security over U.S. Department of Agriculture (USDA) Information Technology (IT) Resources within the Risk Management Agency (RMA). Our overall objective was to assess RMA's information system security program. Specifically, we reviewed the adequacy of security over RMA systems and networks, including logical and physical access controls and controls over the modification of application software programs.

Our audit identified material internal control weaknesses in the overall management and organizational structure for RMA's IT security and operations. We determined that RMA's IT environment is highly vulnerable to errors, misuse, abuse, unauthorized access, disruption of service, and willful destruction. Although management recognized a part of these structural weaknesses prior to our audit, the action taken was neither broad enough in scope nor as aggressive as necessary to achieve acceptable results. For example, although RMA recently hired a Chief Information Officer (CIO), it did not provide the new CIO with sufficient authorities and resources to properly develop and oversee IT operations. We found that RMA's IT organizational structure is under the direct control of production managers, thereby, compromising the integrity and effectiveness of IT security within the organization. In addition, agency senior managers did not establish formally approved agencywide policies and procedures for IT security and operations. RMA also relied on a general reimbursable agreement with the Farm Service Agency (FSA) that did not detail either agencies' expectations or assign authorities and responsibilities for the provided services and that Federal and Department security requirements were complied with. This resulted in unfulfilled responsibilities and unresolved and questioned authorities that contributed to the weak IT program.

Also, RMA breached fundamental security requirements by providing contractors access to a large Federal facility and to USDA IT hardware, systems, and applications without subjecting their contractors to background investigations to determine their suitability for the duties assigned to them. In addition, a Federal employee directly supervised the day-to-day duties and responsibilities of two contracted IT security specialists, in violation of the contract, and RMA did not prepare documentation showing the services expected or provided by these contracted personnel. The contracted security specialists also

performed IT production duties that conflicted with their system security responsibilities.

Our audit, which included electronic vulnerability scans of RMA's systems, identified potentially serious control weaknesses that, if not corrected, could expose RMA's network to internal and external intrusions. Our scans of RMA's network revealed 306 high and medium-risk vulnerabilities that could be exploited, as well as system policy settings that did not provide for optimum security. The likelihood that such access could occur without detection was increased by an inadequate system of firewalls and intrusion detection devices between RMA and the rest of USDA. RMA had acquired similar vulnerability scanning tools but did not scan all systems on a cyclical basis. Also, RMA did not fully develop a configuration management program to ensure that security patches were routinely updated for all systems.

Our vulnerability scans also assessed RMA's network operating settings and found serious and recurring access control weaknesses throughout RMA's networks and systems, including weaknesses in password administration, system administrator accounts, generic or shared user accounts, and accounts with unknown users. We also noted that RMA did not establish effective controls to oversee RMA user accounts on other USDA computer systems. We found significant weaknesses in user account administration, including retention and maintenance of user accounts, user access rights and privileges, and system administrator privileges.

Physical access control components were not in place to safeguard major computer systems and hardware. RMA did not limit physical access to RMA's systems and hardware to only those with an immediate need for access. Although some of the security lapses may, in part, be attributed to weaknesses in building security services provided by the FSA, RMA did not take steps to ensure the adequacy of the services provided or initiate additional controls, where appropriate.

Overall, RMA managers did not adhere to the Department's system development lifecycle (SDLC) methodology for software application development, installation, and/or maintenance. Our review disclosed that RMA had no formal policy or procedures to apply an SDLC process within the agency. Specifically, they did not apply required controls during development and maintenance of one mission critical application we reviewed.

In our judgment, internal control weaknesses exist in RMA, as defined by the General Accounting Office (GAO) “Standards for Internal Control in the Federal Government” and include (1) inappropriate IT organizational structure and resulting environment, (2) absence of approved agencywide policies and procedures for key RMA IT security and production operations, (3) absence of properly prepared RMA vulnerability assessments, (4) ineffective access controls for RMA’s IT systems and networks, (5) physical security weaknesses for access to RMA IT hardware and equipment, and (6) lack of implementation of the Department’s SDLC methodology, which includes controls over major renovations to RMA systems. As material weaknesses, these conditions should be included in the RMA’s Federal Manager’s Financial Integrity Act (FMFIA) report.

## **Recommendations in Brief**

We recommend that the RMA Administrator:

- Include the IT internal control weaknesses in the agency’s FMFIA report;
- Provide sufficient authorities and resources to the CIO to develop and oversee an effective IT system, organization, and operation and reorganize RMA’s IT organization structure to ensure independence of the CIO and the IT security staff from control and undue influence by internal agency production units;
- Renegotiate and revise the reimbursable agreement with FSA to reflect the planned changes in RMA’s IT organizational structure and internal operations and sufficiently detail the expectations, requirements, and services to be provided;
- Immediately develop, document, and implement appropriate written policies and procedures that have been reviewed and approved by responsible senior management covering all RMA IT security operations, processes, functions, and activities and include these policies in handbooks to be provided and used by all managers, system administrators, security officers, developers, contractors, and IT users;
- Prescribe and apply effective management controls, such as periodic monitoring reviews to ensure that approved policies and procedures for RMA IT operations, processes, functions, and activities are properly and consistently applied and continuously enforced agencywide;

- Conduct continuous IT security scans on RMA networks and systems, and require IT managers to establish a configuration management program for RMA's systems;
- Strengthen senior management oversight and periodically monitor the effectiveness of agencywide policies, procedures, and management controls to ensure that contract provisions for IT services conform to all applicable laws and regulations and that all contract provisions are enforced;
- Require background investigations for all IT contractor employees and associated subcontractor employees before access to RMA systems, hardware, and facilities are authorized;
- Establish management controls to ensure that Federal employees do not supervise the day-to-day activities of contracted security specialists and other IT contractor employees and separate duties and responsibilities assigned to individual contractor employees;
- Take immediate action to eliminate the high and medium-risk vulnerabilities identified by our scans, rerun the scans to ensure the vulnerabilities have been corrected, and assess the low-risk vulnerabilities for trends;
- Terminate dial-in access for generic accounts and unidentified users;
- Develop and apply a policy to conduct a routine and timely review of RMA's Kansas City, Missouri, and Washington D.C., firewall configuration;
- Effectively control physical access to RMA IT system hardware and equipment;
- Prescribe and implement a formal directive system on SDLC methodology and system change control directions on an agencywide basis;
- Inform responsible RMA staff of deficiencies cited and corrective action planned or initiated and hold senior managers accountable for corrective action implementation; and
- Report quarterly to the Office of the Chief Information Officer (OCIO) until the reported issues are corrected.

**Agency Response** RMA provided written comments, dated April 14, 2004, to the official draft report, which indicated that RMA conditionally concurred with most of the audit findings and recommendations. RMA's response shows the agency plans aggressive actions to improve the current IT environment. See exhibit B for the RMA written response to the draft report.

**OIG Position** Although RMA's written comments presented conditional concurrence with most findings and recommendations, the comments did not provide sufficient information to reach management decision, except for Recommendation No. 19. To reach management decision for the remaining recommendations in the report, RMA needs to identify the specific actions that will be taken and the estimated timeframes for implementation.

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

---

ADP	Automated Data Processing
ASD	Administrative Services Division
BCCP	Business Continuity and Contingency Plan
CFR	Code of Federal Regulations
CIO	Chief Information Officer
DM	Departmental Manual
DR	Departmental Regulation
F&ITO	Financial and Information Technology Operations
FCIC	Federal Crop Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FMFIA	Federal Manager's Financial Integrity Act
FSA	Farm Service Agency
FY	Fiscal Year
GAO	General Accounting Office
GPRA	Government Performance and Results Act
GSA	General Services Administration
ID	Identification
ISSPM	Information System Security Program Manager
IT	Information Technology
LAN	Local Area Network
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCFO	Office of Chief Financial Officer
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
RMA	Risk Management Agency
SAB	Systems Administration Branch
SCITO	Service Center Interagency Support Operations
SDLC	System Development Lifecycle
SNMP	Simple Network Management Protocol
SP	Special Publication
TCP/IP	Transmission Control Protocol/Internet Protocol
USDA	United States Department of Agriculture
WAN	Wide Area Network
WDC	Washington office located in the District of Columbia



# Table of Contents

---

Executive Summary .....	i
Abbreviations Used in This Report.....	vi
Background and Objectives.....	1
Findings and Recommendations.....	4
<b>Section 1. IT Organizational Structure and Environment.....</b>	<b>4</b>
Finding 1    Management and Organizational Improvements are Needed to Assure a Stronger and More Effective IT Environment .....	4
Recommendation No. 1.....	10
Recommendation No. 2.....	10
Recommendation No. 3.....	11
Finding 2    Approved Policies and Procedures are Needed to Safeguard IT Resources and to Improve Operational Practices .....	11
Recommendation No. 4.....	14
Recommendation No. 5.....	15
Finding 3    RMA Compliance with Federal IT Security and Control Requirements Needs Improvement .....	15
Recommendation No. 6.....	24
Recommendation No. 7.....	24
Recommendation No. 8.....	25
Finding 4    Improved Contract Administration is Needed to Assure Effective IT Security.....	25
Recommendation No. 9.....	29
Recommendation No. 10.....	29
Recommendation No. 11.....	30
Recommendation No. 12.....	31
Finding 5    System Scans are Needed for Effective IT Security Management .....	31
Recommendation No. 13.....	35
Recommendation No. 14.....	36
Recommendation No. 15.....	37
Recommendation No. 16.....	37
Recommendation No. 17.....	38
<b>Section 2. Security Program Management of Information Technology Resources.....</b>	<b>39</b>
Finding 6    Improvements are Needed in Network Operating System Policies and Procedures .....	39
Recommendation No. 18.....	42
Recommendation No. 19.....	43

Finding 7	Stronger Controls are Needed to Restrict Access to RMA Systems and Networks .....	44
	Recommendation No. 20.....	50
	Recommendation No. 21.....	50
	Recommendation No. 22.....	51
	Recommendation No. 23.....	51
	Recommendation No. 24.....	52
	Recommendation No. 25.....	53
Finding 8	Stronger Physical Security is Necessary for Shared IT System Hardware and Facilities .....	54
	Recommendation No. 26.....	56
	Recommendation No. 27.....	57
	Recommendation No. 28.....	57
<b>Section 3. Application Controls and Tests .....</b>		<b>59</b>
Finding 9	Implementation of the System Development Lifecycle Methodology Would Improve Security and Performance .....	59
	Recommendation No. 29.....	63
Finding 10	Agencywide System and Application Change Controls are Needed .....	64
	Recommendation No. 30.....	68
	Recommendation No. 31.....	68
	Recommendation No. 32.....	69
	Recommendation No. 33.....	69
	Recommendation No. 34.....	70
<b>Scope and Methodology.....</b>		<b>71</b>
<b>Glossary of Terms.....</b>		<b>73</b>
<b>Exhibit A – RMA IT Organizational Chart .....</b>		<b>75</b>
<b>Exhibit A – Key to RMA IT Organizational Chart.....</b>		<b>76</b>
<b>Exhibit B – RMA Response to the Draft Report.....</b>		<b>77</b>

# ***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 enhanced the ability to share information instantaneously among computers and networks, it also made organizations more vulnerable to unlawful and destructive penetration and disruptions. Risk Management Agency's (RMA) information systems perform critical functions for program delivery and about 650,000 crop insurance program participants rely on the systems for integrity and general support.

Various laws emphasize the need to protect agencies' sensitive and critical data, particularly the Privacy Act of 1974 and the Computer Security Act of 1987. Information security responsibilities were reemphasized in the Clinger-Cohen Act of 1997 and Presidential Decision Directive 63.<sup>1</sup> The Government Information Security Reform Act (October 2000) codified existing requirements of the Office of Management and Budget (OMB) Circular A-130.<sup>2</sup> In addition, the National Institute of Standards and Technology (NIST)<sup>3</sup> issued several Federal Information Processing Standards (FIPS), 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>4</sup> provides standards, guidelines, and procedures for the development and administration of automated data processing security programs mandated by Departmental Regulations (DR).

The Federal Crop Insurance Reform and Department of Agriculture Reorganization Act of 1994 consolidated the personnel resources of the Federal Crop Insurance Corporation (FCIC), the Agricultural Stabilization and Conservation Service, and parts of the Farmers Home Administration and the Foreign Agricultural Service into the Farm Service Agency (FSA). However, the corporate structure of FCIC remained intact and its program personnel were generally assigned to the FSA Deputy Administrator for Risk Management. At the time of the consolidation, about 40 FCIC IT positions were transferred to FSA,

---

<sup>1</sup> Presidential Decision Directive 63, "Policy on Critical Infrastructure Protection" (May 1998).

<sup>2</sup> OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" (November 2000).

<sup>3</sup> The Computer Security Act of 1987 assigned NIST primary responsibility for developing technical standards and providing related guidance. Their responsibilities were reemphasized in Section 2.B1 of the Clinger-Cohen Act of 1997.

<sup>4</sup> DM 3140-1, "Management ADP Security Manual" (July 1984), Part 1 of 8, Section 1.

including the Information Resource Management Director, the equivalent of RMA's Chief Information Officer (CIO).

On April 4, 1996, the Department of Agriculture Reorganization Act (Public Law 104-127, Title II) was amended to establish an agency within the Department, separate from FSA, to supervise FCIC administration and programs. On May 3, 1996, the Secretary issued a memorandum establishing the RMA. Under this memorandum, FSA retained FCIC's portion of the combined agencies' administrative structure, including IT security and operations. In return, RMA lost key IT personnel resources, formerly held by FCIC, to FSA, including RMA's CIO and security officer positions. On January 7, 2004, the RMA Administrator explained that FSA fulfilled RMA's CIO responsibilities from 1996 to April 2003. In 1996, FSA and RMA initiated a series of reimbursable agreements for the administrative and IT services provided to RMA by FSA. The terms of the agreements were generally stated and did not specifically address FSA or RMA CIO responsibilities. Prior to our audit, RMA requested Departmental approval to hire a CIO for RMA's IT operations and activities. The request was approved and RMA hired a CIO in April 2003.

RMA administers Federal crop insurance programs through 17 commercial insurance companies that are also supported by a network of 15,000 agents who sell crop insurance policies and provide front-line information on the latest programs available to producers. RMA works with its public and private partners to find improved risk management strategies, develop educational curricula and materials, and train producers in effective use of risk management tools.

RMA maintained three mission-critical applications during the period of our audit. RMA's system documentation indicated that each of these applications processed sensitive data. One of the three applications supported sales and program administration activities by insurance providers and their agent and was used by RMA to support other applications. The application did not process financial data but processed about 235,000 pages of documents each year. RMA used a second application to test program and financial data transmitted from reinsurance companies before the data were accepted and distributed to downstream feeder systems or databases, as appropriate. The third mission-critical application tracked financial activity and produced monthly summary financial reports for distribution to the reinsurance companies. The second and third applications processed financial data totaling almost \$7 billion (total premiums plus indemnities) for the 2002 crop year.

The Federal Manager's Financial Integrity Act (FMFIA) requires that agencies evaluate their systems of management controls and report any material weaknesses identified. In its fiscal year (FY) 2002 report to Congress, RMA reported that it had no material weaknesses and the management control systems generally complied with the FMFIA.

In November 2001, RMA received the results from a contractor's performed evaluation entitled "Review and Assess Current RMA Business Process Practices." The document is the deliverable analysis and assessment report on RMA's current business and system processes, rules, practices, and process models for the Emerging Information Technology Architecture. In part two of four parts, the report cites critical factors for RMA and major IT problem areas that will need attention if RMA is to make significant strides under any business practice mode. Some identified issues include (1) an ineffective top-down planning and direction for IT and (2) a resource intensive approach to IT systems, including inadequate software development processes. These documents were to be the support for the subsequent development of a 5-Year Information Technology and Change Management Plan for RMA.

The USDA Office of Inspector General (OIG), Financial and Information Technology Operations (F&ITO), conducted nationwide audits of selected USDA agencies to assess the overall management and security of major USDA computer systems. RMA was one of several agencies selected for review as part of the nationwide audit of USDA mission-critical systems. F&ITO will issue a nationwide audit report to the Office of Chief Information Officer (OCIO).

## **Objectives**

The objectives of this audit were to (1) assess the overall management of RMA's Information System Security Program, (2) determine the adequacy of the security over the local and wide area networks, and identify vulnerabilities in Departmental payment/data systems, (3) determine if adequate logical and physical access controls exist to protect computer resources against unauthorized modification, disclosure, loss, or impairment, (4) evaluate the controls over the modification of application software programs to ensure that only authorized modifications were implemented, and (5) determine the adequacy of controls over access to and modification of system software and data transmission.

# Findings and Recommendations

## Section 1. IT Organizational Structure and Environment

---

Our audit identified serious weaknesses in RMA's management and organizational structure for IT operations. We found (1) RMA's IT organizational structure is detrimental to a strong IT security program because authority and responsibility for all critical IT systems and operations, including system security, was held by a program manager who was also responsible for handling critical programs and/or IT production operations, (2) RMA did not establish formal agencywide IT policies and procedures, (3) RMA did not comply with federally mandated security guidelines, (4) RMA did not administer a contract for IT services in accordance with applicable Federal requirements or the provisions of the contract, and (5) RMA has systemic weaknesses in access controls. These conditions existed primarily because production operations were emphasized by program managers instead of effective security and controls. RMA management took action to initiate improvements during our audit; however, the actions were neither broad enough in scope nor as aggressive as necessary to achieve a reliable IT environment. The RMA Administrator advised us that they have been constrained from taking all their contemplated actions until their proposed reorganization plan has been approved by the Department. As part of the proposed reorganization, RMA did initiate action to employ its own CIO prior to our audit. The CIO was hired during our audit and began to propose changes in the IT structure. However, much work remains before RMA succeeds in establishing IT oversight that is independent of production manager direction. As a result, the IT environment was generally void of written agencywide policy and procedures, did not comply with applicable Federal laws and regulations, and was inefficient and ineffective in safeguarding RMA IT resources as well as sensitive financial and program data.

---

### Finding 1

### **Management and Organizational Improvements are Needed to Assure a Stronger and More Effective IT Environment**

Although RMA management initiated action to improve its IT organizational structure, we found that key elements of the structure, such as independent IT management, an adequate reimbursable agreement, and separation of duties, were either (1) missing, (2) did not conform to NIST's<sup>5</sup> "Generally Accepted Principles and Practices for Securing Information Technology Systems," and/or (3) did not comply

---

<sup>5</sup> NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems" (September 1996).

with OMB Circular A-130, Appendix III. We concluded that the conditions existed because production operations were emphasized over effective security and controls. As a result, these conditions jeopardize the security of critical RMA IT system networks and operations, as well as critical and sensitive financial and program data.

A. Independent IT Management. RMA delegated responsibility for all critical IT systems and operations, including systems security, to a program manager who was also responsible for ensuring that RMA's goals were achieved in critical program areas, such as actuarial operations, product development, research and evaluation, and fiscal operations. Exhibit A presents an abbreviated IT organizational chart as of January 1, 2003. It shows an acting CIO that was separated from general IT responsibilities and authorities (see block A1 of exhibit A). In April 2003, RMA hired a CIO who was to be aligned under the RMA Administrator, independent of program managers, but his responsibilities and authorities have not yet been fully determined. In the interim, all critical IT systems and operational components remained aligned under the program manager.

GAO's "Federal Information System Controls Audit Manual" states, *"An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources."*<sup>6</sup>

NIST SP 800-12<sup>7</sup> advises that: *"A natural tension often exists between computer security and operational elements. In many instances, operational components -- which tend to be far larger and therefore more influential --- seek to resolve this tension by embedding the computer security program in computer operations. The typical result of this organizational strategy is a computer security program that lacks independence, has minimal authority, receives little management attention, and has few resources. As*

---

<sup>6</sup> GAO "Federal Information System Controls Audit Manual" (January 1999).

<sup>7</sup> NIST SP 800-12, "An Introduction to Computer Security," Section 6.5.

*early as 1978, GAO identified this organizational mode as one of the principal basic weaknesses in Federal agency computer security programs.”*

The number of high-level risks associated with the following conditions can be directly attributed to RMA’s IT environment and organizational structure. We found:

- An absence of senior management approved written policies, procedures, and directives for IT operations, including mandatory security policies and procedures (see Finding No. 2);
- A pattern of noncompliance with Federal IT security guidelines (see Finding No. 3);
- Inappropriate administration of major IT service contracts (see Finding No. 4);
- Inadequate controls to prevent unnecessary and unauthorized access to IT systems and equipment (see Findings Nos. 5 through 8); and
- Noncompliance with requirements for periodic systems reviews, system software development and maintenance reviews, and software testing procedures (see Findings Nos. 9 and 10).

In addition, we noted a contractor, procured by RMA for an independent review of its IT operations, also cited weaknesses in RMA’s CIO structure and ineffective top-down planning and direction for IT in a report, dated November 15, 2001. This report also contained a recommendation that RMA establish a full-fledged CIO organization empowered to ensure that IT needs are addressed on the basis of their business urgency and impact. RMA took limited corrective action on the contractor’s report, the most significant of which was hiring a CIO, even though they had not yet defined the CIO’s responsibilities, authorities, and duties.

We discussed this issue with responsible RMA officials and they generally agreed with the cited conditions. We believe that RMA should act promptly to separate control of IT operations from production manager’s responsibilities and provide RMA’s new CIO with sufficient resources and managerial support to develop a secure, productive, documented, and effective IT environment.



B. RMA - FSA Reimbursable Agreement. After a 2-year consolidation with the FSA ended in 1996, RMA relied on FSA to perform certain administrative functions, including IT security and certain network administration operations. These services were provided through a series of reimbursable agreements, the latest of which was approved for FY 2001. The 2001 agreement was extended, without revision, for FY's 2002 and 2003. The terms of the agreement were generally stated, without details of either agency's expectations for the provided services. The absence of detailed expectations for both agencies has resulted in unfulfilled responsibilities and unresolved questioned authorities that have contributed to a weak IT program. For example, the reimbursable agreement did not provide specifics, such as whether or not the FSA would fulfill RMA CIO responsibilities since RMA did not have a CIO in place. The agreement did not contain specific information for performing key security operations, which contributed to compromising the integrity of RMA's IT operations and security. We found that the potential existed for unnecessary and unauthorized access to RMA IT systems and equipment.

Also, confusion existed within both RMA and FSA about how RMA's Security Officer's responsibilities and duties fit into the IT organizational structures of both agencies (block X1 in exhibit A). The RMA Security Officer is an FSA employee who worked for FCIC before the agencies were combined in 1994. Although there was no specific reference to the Security Officer in the reimbursable agreement, the position was clearly covered by the agreement. As an FSA employee, the RMA Security Officer reported directly to the FSA Security Officer in Kansas City, Missouri. However, the FSA Security Officer (block B3a in exhibit A) stated that the RMA Security Officer did not report to him for daily assignments; he only provided the RMA Security Officer with an annual performance appraisal and did not actively supervise the RMA employee's day-to-day activities. The appraisals were based on comments provided by an RMA program division chief.

We interviewed the RMA Security Officer and she concurred that she was often in an awkward position because program priorities often conflicted with security requirements. We found that the Security Officer took direction primarily from an RMA program division chief.

We also noted that the contractor who conducted a review of RMA IT operations also cited weaknesses in RMA's reimbursable agreement and FSA's help desk support function. The report states

RMA funds FSA to provide help desk and local area network (LAN) support to its entire contingent of desktop systems plus the LAN. Yet, the agreement “*contains virtually none of the service level specifications one would normally expect to see governing such an arrangement.*” Specifically, the contractor’s report recommended that RMA establish a clear service level agreement with FSA governing the level of Desktop support expected.

Recent activities indicate that RMA has proposed to control all of its IT resources and limit or terminate any FSA responsibility for RMA IT security and operations. However, this change must be accomplished with Departmental approval and RMA has not yet submitted a request to make the necessary organizational changes to the Department. In the interim, RMA and FSA should revise or enter into a new reimbursable agreement that clearly defines the expectations, responsibilities, and duties of both agencies for all IT personnel and services to be provided under the agreement.

- C. Separation of Duties. Our audit disclosed several specific situations where key RMA IT personnel held conflicting and/or incompatible duties and responsibilities. Specifically, the RMA Security Officer (an FSA employee who reported directly to an RMA employee, see block X1 in exhibit A) was actually supervised by an RMA production manager (see block A2c1 in exhibit A). Also, one RMA employee authored and controlled the source code of a mission-critical accounting application throughout its development and life cycle. The programmer created the computer code for the application, then tested it, then moved it through the development and testing phases and into production, and then maintained the code while the application was used for production. We also noted two contracted security specialists who also had conflicting duties (blocks CX1 and CX2 in exhibit A), in that each contractor worked on both system security and key production projects (see Finding No. 4).

OMB Circular A-130, Appendix III,<sup>8</sup> requires agencies to incorporate controls, such as separation of duties, least privilege, and individual accountability into the application and application rules, as appropriate. Key duties and responsibilities include authorizing, recording, and reviewing official agency transactions and should be separated among individuals.

In the first situation, the RMA Security Officer is an FSA employee who reported directly to the Chief, System Administration Branch (see block A2e in exhibit A). The Branch

---

<sup>8</sup> OMB A-130, Appendix III (November 2000), Subpart A3b.2c.

Chief and the Security Officer were a part of RMA's program staff. In order to effectively provide security services, the Security Officer must be independent of interference and influence of production managers. Direct supervision of the Security Officer by a production manager is not compatible with guidance provided in NIST SP 800-12<sup>9</sup> or with internal control standards for separation of duties.

General Accounting Office (GAO) Federal Information Systems Control Audit Manual states different individuals should generally perform the following functions; system design, application programming, data security, and network administration.

Also, we found that one RMA employee (1) created all the source code for Application E, one of RMA's critical systems, (2) tested and moved Application E into production without technical oversight or quality assurance review, (3) conducted subsequent maintenance on the source code for Application E without technical oversight or quality assurance review, and (4) was the owner of the directory where production source code for Application E was maintained.

The responsible program manager explained that this occurred because the employee was proficient with the programming package used for the application and possessed the accounting knowledge needed to develop the code. As a result, Application E is highly vulnerable to intentional and unintentional errors, misuse, abuse, unauthorized access, disruption of service, and willful destruction.

Shortly after our interviews, the Branch Chief began to reorganize personnel assignments for Application E. The manager provided a draft revision of assignments for accounting systems that listed two other computer specialists as the primary and secondary contacts for Application E. The employee who originally created, tested, maintained, and put Application E into production was to be reassigned as the primary system accountant for the application. We noted, however, that the employee remained the primary contact and maintained the application's source code throughout the period of our review.

---

<sup>9</sup> NIST SP 800-12, Section 6.5.

## **Recommendation No. 1**

Delegate sufficient authorities and provide adequate staff and other resources to the CIO to develop and oversee an effective IT system, organization, and operation, and to properly manage and administer RMA IT security activities.

### **RMA Response.**

“RMA conditionally concurs. Senior Management has reviewed current IT authorities and resources. A draft proposal addressing this recommendation is currently under review. OIG and the OCIO will be provided with the document once approved.”

### **OIG Position.**

Although RMA’s written comments presented conditional concurrence, they did not provide sufficient information to enable us to accept management decision for the recommendation. To reach management decision, RMA needs to identify the specific actions that will or have been taken, the adequacy of the contents of the proposal, and the estimated timeframes for implementation of the proposal.

## **Recommendation No. 2**

Reorganize the RMA’s IT organization structure to ensure the independence of the CIO and the IT security staff from control and improper influence by production managers.

### **RMA Response.**

“RMA conditionally concurs. Senior Management is analyzing the current IT organizational structure, including issues related to the CIO and security staff. A draft proposal will be issued for review in the near future. The document will be distributed to OIG and the OCIO once approved.”

### **OIG Position.**

Although RMA’s written comments presented conditional concurrence, they did not provide sufficient information to enable us to accept the management decision for the recommendation. To reach management decision, RMA needs to identify the specific actions that will or have been taken, related to the CIO and security staff, regarding control and improper influence by production managers and the estimated timeframes for implementation of the proposal.

### Recommendation No. 3

Renegotiate and revise the reimbursable agreement with FSA to reflect planned changes in RMA's IT organizational structure and internal operations. The agreement should include sufficiently detailed descriptions of the services to be provided so that the IT responsibilities of both agencies are clearly understood by the employees charged with carrying them out, as well as by agency managers, employees, and other parties, as needed.

#### **RMA Response.**

"RMA concurs. As discussed during the audit, FSA is currently divesting itself of all interagency support functions as part of the move to the service center (SCITO).<sup>10</sup> RMA is currently negotiating with FSA regarding the return of functions, personnel, and budget. RMA has rewritten the Memorandum of Understanding for renegotiation in the event SCITO negotiations are cancelled."

#### **OIG Position.**

Although RMA's written comments presented concurrence, they did not provide sufficient information to enable us to management decision for the recommendation. To reach management decision, RMA needs to provide a detailed description on the specific actions that will or have been taken and the estimated timeframes for implementation the corrective actions.

---

#### **Finding 2**

#### **Approved Policies and Procedures are Needed to Safeguard IT Resources and to Improve Operational Practices**

RMA did not establish and document its agencywide policies and procedures for IT security and operations. This occurred primarily because RMA did not manage its IT resources under an organizational and management structure that clearly delegated policy and procedural authorities and responsibilities to an independent IT manager or CIO. As a result, RMA cannot provide reasonable assurance (1) that employees and contractors who performed RMA's day-to-day IT operations understood how, when, where, why, and by whom necessary duties or tasks should be performed, (2) that RMA's IT security and production operations complied with applicable laws and regulations,

---

<sup>10</sup> "SCITO" is an acronym for "Service Center Interagency Support Operations."

or (3) that RMA's IT security and production operations operate as intended. The absence of approved policies and procedures also significantly increases the vulnerability of RMA's IT resources and is detrimental to a strong information systems security program.

GAO "Standards for Internal Control in the Federal Government"<sup>11</sup> states: *"In implementing these standards, management is responsible for developing the detailed policies, procedures, and practices to fit their agency's operations, and to ensure that they are built into and an integral part of operations."* The Control Environment Standard states, *"Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management."* Supporting narrative further explains *"A positive control environment is the foundation for all other standards."*

NIST SP 800-12<sup>12</sup> states that new technologies and the appearance of new threats often require the creation of issue-specific policies. Potential candidates for issue-specific policy include protection of proprietary information, unauthorized software, encryption of files, and e-mail.

Our audit disclosed an almost complete absence of formally approved policies and procedures by RMA senior management for IT security and operations. We also found instances where draft procedures were developed, but were neither approved nor disapproved by senior management, and instances where managers took it upon themselves to issue informal procedures to their staffs. For example, the IT Security Officer developed draft IT security policies and procedures but no responsible senior RMA official approved them for implementation. Also, one branch chief used e-mail to distribute informal "desk" procedures for controlling software change requests to his staff. These procedures were not approved by senior management and, thus, were not consistently applied throughout RMA.

A list of examples of policies that were not developed, or procedures that were developed but not approved by senior management, or were informal "desk" procedures, as of April 2003, follow:

- General IT management and security procedures were unapproved and issued in draft form to employees and contractors. Some unapproved draft procedures were developed by the Security Officer;

---

<sup>11</sup> GAO "Standards for Internal Control in the Federal Government," GAO/AIMD-00-21.3.1 (November 1999), pages 7 and 8.

<sup>12</sup> NIST SP 800-12, Sections 5.2.1 and 5.2.2.

- Incident response procedures were not developed;
- Performance goals and measures were not developed;
- Security vulnerability scan procedures were developed, but not approved;
- Procedures for handling system patches and updates were developed, but not approved;
- General password and user account administration procedures were developed, but not approved;
- Policy prohibiting the loading of software without RMA authorization was not developed;
- Shared and generic user account administration procedures were developed, but not approved;
- System Development Lifecycle (SDLC) Methodology for software development was not developed;
- Application/systems change control “desk” procedures were developed in the absence of approved procedures;
- Procedures for conducting system and application tests, documenting test plans, and approving software maintenance were not developed; and
- Internet and e-mail usage policies and procedures were not developed.

Informal policies and procedures lack the weight of authority provided by the written approval of a senior management official. The signature of a responsible authority provides clear evidence for employees and contractors that management is in agreement with the stated policies and procedures and that adherence to them is required. During the review, we could not identify a RMA manager who had been specifically delegated responsibility for assuring that critical IT policies and procedures were formally approved and in place.

Since FSA employees provide services relating to RMA security, we noted that FSA has a comprehensive “Information Systems Security Program” handbook that provides policies, responsibilities, and controls that could be used as a model by RMA as they develop and

implement adequate policies and procedures to protect their IT information.

#### **Recommendation No. 4**

Immediately develop, document, and implement appropriate written policies and procedures that have been reviewed and approved by responsible senior management covering all RMA IT security operations, processes, functions, and activities and include these policies in handbooks to be provided and used by all managers, system administrators, security officers, developers, contractors, and IT users. The handbooks should provide RMA IT policies, assign IT responsibilities, and identify the management controls that shall be implemented to protect RMA's IT resources and ensure they are functioning as intended.

#### **RMA Response.**

“RMA concurs. However, it should be noted that policies for seven broad IT areas were drafted, distributed and put in place before the audit, however, they did lack the CIO's signature. The policies were approved by two levels of management, put in force, and were being monitored to assure adherence. Violations were reported to the ISSPM (Information System Security Program Manager or Agency Security Officer) and escalated up the management chain (including to the OCIO Office of Cyber Security when appropriate). All that was lacking was the "official" signature of the Administrator or CIO. RMA continues to implement new policies and to conduct regular reviews of current policies.”

#### **OIG Position.**

RMA's written comments showed they concurred and had taken action to issue seven broad IT policies but did not have the official signature of the CIO or Administrator. The comments were positive but did not provide sufficient information to enable us to reach management decision. To reach management decision, RMA needs to provide the estimated timeframes for implementation of the remaining contemplated corrective actions. Also, they will need to provide a detailed description of those IT security operations, processes, functions and activities covered by the cited policies and those still needing inclusion in RMA's directives.



## Recommendation No. 5

Prescribe and apply a periodic monitoring review process to ensure that approved policies and procedures for RMA IT operations, processes, functions, and activities are properly and consistently applied and continuously enforced agencywide.

### **RMA Response.**

“RMA concurs. RMA's CIO, System Administration Chief and Security Officer and staff are systematically analyzing and documenting enforcement mechanisms (automated and manual) for Agency IT policies and procedures. These will be incorporated into the CIO's IT Internal Control Manual. Processes will include recording and retaining checklists, reports, etc., for auditor review beginning in FY 2005.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation, but the comments did not provide sufficient information to reach management decision. To reach management decision, RMA needs to more fully describe the specific enforcement actions to be taken and codified in the CIO IT Internal Control Manual and the process that will be used by senior management to monitor the review process, as well as specific timeframes for implementation of the corrective actions.

---

### **Finding 3**

### **RMA Compliance with Federal IT Security and Control Requirements Needs Improvement**

RMA managers did not administer RMA's IT operations in accordance with applicable laws and regulations. We determined that the absence of an RMA CIO and the resulting alignment of the IT security officer under production managers significantly reduced RMA's ability to comply with the laws and regulations that apply to IT operations and resources. Our audit disclosed areas of significant noncompliance, and we believe the cited conditions could be significantly reduced with a more responsive organizational structure. RMA did not disclose any IT weaknesses in their annual FMFIA reports. As a result of these conditions, the vulnerability of RMA's IT resources to errors, misuse, abuse, unauthorized access, disruption of service, and willful destruction is significantly increased. Furthermore, the results of such noncompliance may impact on almost every element of RMA's program and financial operations, as well as the more general information and services provided to crop insurance program

participants. We found that RMA did not (1) conduct required risk assessments for its three mission-critical systems, (2) certify that its three mission-critical systems met all existing security requirements, (3) develop security plans or properly plan contingencies and disaster recovery, and (4) obtain required security clearances, complete security clearances, effectively implement policies for intrusions, establish IT performance measures, and always prevent loading of unauthorized software on agency computers. We noted during our review that:

A. FMFIA Review Reporting. We reviewed RMA's 2002 FMFIA report and assessments and found that RMA's assessments were not effective in identifying internal control weaknesses for that period. For example, the FMFIA assessment for the security plan for the LAN/wide area network (WAN) infrastructure states that the LAN administrator access is provided on a need-to-know basis. RMA's answer was incorrect as to who had administrator access on this system. RMA officials believed that six to seven people had LAN administrator access, including both FSA employees and contractors. Additionally, in January 2003, RMA officials stated there was a file that contained administrator access ID's (identification) and passwords that were accessible by 12 people. Our system security scan identified 112 people with access rights to this file. RMA was unaware of the additional 100 people with access rights to this file.

The FMFIA requires agency heads to report material internal control weaknesses of their internal administrative and financial management systems. Based upon the cumulative potential impact of management control weaknesses found during the audit and lack of compliance with Federal laws, regulations, and Departmental requirements, as well as GAO's "Standards for Internal Control in the Federal Government," we believe the following conditions should be included in the RMA's current FMFIA reports:

- RMA's fragmented IT organizational structure and resulting IT management control environment;
- The absence of senior management approved agencywide policies and procedures for key RMA IT security and production operations;
- The absence of properly prepared RMA vulnerability assessments and mission-critical certifications;
- Ineffective access controls for RMA's IT systems and networks;

- Physical security weaknesses for access to RMA IT hardware and equipment; and
  - RMA's failure to implement the Department's SDLC methodology, which includes controls over major renovations to RMA systems.
- B. Risk Assessments. RMA did not conduct or approve detailed risk assessments for its three mission-critical systems, based on the critical applications used to perform the business processes, as required by NIST and OMB. This occurred because IT managers believed that other documentation already fulfilled this requirement. We reviewed abbreviated risk assessments that RMA incorporated in the Business Continuity and Contingency Plan (BCCP) that were based on RMA core business processes but they did not contain the required information on critical applications. Management also provided a draft risk assessment for one mission-critical system that was not yet approved by senior management. The officials stated that the assessments for the two remaining mission-critical systems were in draft form but were also not yet approved by senior management. Risk assessment methodology is applicable to all USDA IT systems, general support, or major applications, as well as systems that are classified and unclassified.

As an example of the potential impact of effective risk assessments, we believe that RMA's need for background investigations for key IT positions (see detail F of this finding) would be identified during a well-designed assessment process and the weakness promptly corrected. Without properly completed and approved risk assessments, RMA cannot provide assurance that risks for mission-critical applications were properly identified, analyzed, and corrected.

OMB Circular A-130<sup>13</sup> states that a risk-based approach is needed to determine the adequacy of RMA's security requirements. This approach should include a consideration of the major factors in risk management; the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. NIST SP 800-30 also states that risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the potential threat and the risk associated with an IT system<sup>14</sup> throughout its SDLC. The

---

<sup>13</sup> OMB Circular A-130, Appendix III (November 2000), Section B.

<sup>14</sup> NIST SP 800-30, "Risk Management Guide for Information Technology Systems" (October 2002), Section 1, defines IT systems as a general support system or a major application that can run on a general support system.

publication also states that the risk assessment process should be repeated at least every 3 years.

- C. Certification. RMA did not certify or otherwise authorize RMA's three mission-critical business applications. Without adequate certification and accreditation of RMA's mission-critical systems, RMA cannot assure that adequate security controls were established for the systems or that existing controls operate effectively. In our opinion, the absence of authorizations or certifications has sufficient negative impact on the security of critical systems to warrant inclusion in RMA's FMFIA report.

OMB Circular A-130<sup>15</sup> states that the accreditation of a system to process information, granted by a management official, provides an important quality control. Management accreditation should be based on an assessment of management, operational, and technical controls. Certification refers to security reviews or evaluations, formal or informal, which take place prior to and are used to support accreditation. Since the security plan establishes the security controls, it should form the basis for the accreditation, supplemented by more specific studies, as needed. In addition, the periodic review of controls should also contribute to future authorizations.

One of the three applications supported sales and program administration activities by insurance providers and their agents and was used by RMA to support other applications. A second application was used to test program and financial data transmitted from reinsurance companies before the data were accepted and distributed to downstream feeder systems or databases, as appropriate. The third mission-critical application tracked financial activity and produced monthly summary financial reports for distribution to the reinsurance companies. The second and third applications processed financial data totaling almost \$7 billion (total premiums plus indemnities) for the 2002 crop year.

For example, an RMA checklist used to document an assessment of one of the three mission-critical applications contained the following question: *"Has a Certifying Official formally certified, in writing, that the system meets applicable Federal policies, regulations, and standards."* The assessing reviewer properly recorded the answer as "No." We discussed the negative answer with responsible RMA officials and they concurred that the systems had not been certified in the past. They also believed that

---

<sup>15</sup> OMB Circular A-130, Appendix III (November 2000), Subsection Ba4.

certifications were a recent requirement. However, guidance for computer security certification and accreditation was established as far back as September 1983 (FIPS 102).

- D. Security Plans. While RMA prepared security plans for systems (Systems A and B) located in Kansas City, Missouri, it did not develop plans for a shared network located in Washington, D.C. (WDC). RMA identified three mission-critical system applications in its “Overall Security Plan” but did not prepare security plans for the applications (Applications D and E). RMA did not perform periodic security control reviews or risk assessments for the applications. As a result, there was no assurance that the security plans were updated, certified, and approved for these applications that process sensitive information.

The Computer Security Act requires agencies to develop security plans for Federal computer systems that contain sensitive information. OMB Circular A-130<sup>16</sup> also requires agencies to prepare security plans for general support systems and major applications to provide an overview of the security requirements of their systems. Security plans should define the persons who were responsible for system security or have authority to access the system and provide appropriate limits on interconnectivity with other systems and security training of individuals authorized to use the system. RMA officials agreed that security plans were needed for their systems and applications.

- E. Contingency Planning and Disaster Recovery. RMA did not prioritize critical data and operations because management did not complete the required risk assessments for mission-critical systems. RMA managers did not identify the resources that support the operations and did not establish emergency priorities. Without an adequate IT contingency plan, RMA cannot be assured that its network and operations can recover quickly and effectively to accomplish its mission in the event of an emergency.

NIST SP 800-34<sup>17</sup> states that Business Impact Analysis is a key step in the contingency planning process. The analysis should include identification of critical IT resources, disruption impacts, allowable outage times, and development of recovery priorities. Effective risk assessments would help RMA identify risks associated with each mission-critical system and the resources necessary to continue operating the systems during emergencies. Without knowing the level of risk associated with each system,

---

<sup>16</sup> OMB Circular A-130, Appendix III (November 2000), Subsection Ba3.

<sup>17</sup> NIST SP 800-34, “IT Contingency Planning – Guidance” (December 2001), Section 3.2.

managers cannot properly establish emergency priorities to continue to meet their mission when disruptions occur.

RMA officials believed that the data and operations were prioritized in RMA's BCCP and that the priorities continually change, based upon the operational priorities regarding RMA's position in its monthly processing. However, we found no prioritization of data and operations in the BCCP and concluded that the order for restoration of system and application data and operations remains unclear in the event of a disaster.

- F. Background Investigations. Security clearances of RMA employees and contractors, including those with significant administrative responsibilities for IT resources or access to sensitive data, were either not accomplished, were not timely updated, or were not adequate when performed. Interviews with RMA administrative and security officials disclosed that RMA did not perform security clearances for employees or contractors. Furthermore, RMA did not have procedural requirements to ensure that employees and contractors in sensitive positions were subjected to appropriate background investigations. One official stated that investigations were not requested, due to limited funding available for the task and management's opinion that RMA did not deal with sensitive information. As a result, RMA has allowed employees and contractors access to critical systems and sensitive agency data, although some personnel may be unsuitable for such positions.

Federal Regulations<sup>18</sup> and OMB Circular A-130<sup>19</sup> require that persons in positions of public trust and those who are authorized to bypass significant technical and operational security controls have periodic background investigations. DR 3140<sup>20</sup> requires personnel, including contractors, working in the automated data processing (ADP) environment to have proper personnel security clearances.

Our review of 12 Kansas City, Missouri, employee personnel folders disclosed that 6 contained no information on security clearances. One of these employees was the RMA IT Security Officer and another was a manager who previously supervised the Security Officer. The Security Officer confirmed that she had not been subject to a background investigation or a security clearance process. Background investigations were performed on the remaining six employees for non-critical/non-sensitive positions.

---

<sup>18</sup> Title 5, Code of Federal Regulations (CFR), Section 731.106.

<sup>19</sup> OMB Circular A-130, Appendix III (November 2000), Subsection B.a.2b.2c.

<sup>20</sup> DR 3140-0001, "USDA Information Systems Security Policy," Subsection 10.d(5).

Five of these six investigations were not updated within the required maximum 10-year interval.

The personnel folders of 13 selected WDC employees disclosed no evidence of background investigations for 3 employees. The folders for seven employees indicated that background investigations had been performed, but three of these were not updated within the 10-year time limit. Three other RMA officials held top-secret clearances with up-to-date background investigations.

- G. Incident Response Procedures. RMA did not develop procedures or effectively implement USDA policy and procedures for reporting and responding to intrusions and attempted intrusions into RMA's IT systems. USDA policy and procedures were developed to ensure that security incidents at USDA (including FSA and RMA, among others) were tracked and adequate corrective actions were taken to prevent recurrence. RMA managers acknowledged that they were aware of "denial of services" attacks on agency IT systems in the past. The managers stated that they follow the USDA policy for incident response, but employees did not complete necessary documentation, due to a lack of available staff and time. As a result, we were unable to determine the number and type of security incidents incurred by RMA and whether they were reported according to Departmental requirements.

The OCIO Cyber Security Office issued the "USDA Computer Incident Reporting Procedure" (October 2001); the procedure requires USDA agencies to develop procedures to report and respond to intrusions and attempted intrusions. At a minimum, the procedures should include an appropriate reporting chain, involvement of the Security Officer, preservation of evidence, containment actions, documentation, and identification of corrective actions taken to strengthen USDA security programs.

The USDA policy provides detailed descriptions of the appropriate contact points, the responsibilities of RMA, and the reporting and documentation requirements that must be met in the event of an incident. However, we found RMA managers did not maintain a log of security incidents and relied on e-mail exchanges among responsible parties for incident response documentation. However, RMA did not incorporate e-mail as acceptable documentation for the incident response reporting system. The security staff described one intrusion incident that occurred while the Security Officer was out of the office. The staff could not recall the date of

the incident and did not record how, or by whom, it was discovered. The staff stated that FSA security personnel conducted the investigation and did not forward documentation of the incident or the investigation to RMA. As a result, RMA's Security Officer was not aware of the cause of the intrusion and could not apply appropriate corrective action to prevent similar incidents from recurring. These circumstances provide little assurance that intrusion incidents were properly addressed in the past or will be in the future.

- H. Security Training. RMA did not provide training or prepare documentation showing that about 360 agency employees and contractors received mandatory annual computer security awareness training during calendar year 2002, as required. RMA also did not maintain documentation showing that personnel with significant administrative responsibilities over IT resources were provided specialized technical training commensurate with their duties and responsibilities, including RMA's IT program managers and Security Officer. The agency did not issue approved procedures requiring users (employees and contractors) to attend annual computer security training in accordance with Departmental regulations. Documentation of training is necessary to assure that all appropriate employees and contractors receive mandatory training and that RMA adheres to applicable training requirements.

The Computer Security Act of 1987<sup>21</sup> requires agencies to provide annual training to employees who are involved with the management, use, or operation of each Federal computer system. The mandatory training should include at least computer security awareness and accepted security practice. In addition, DR 3140-001<sup>22</sup> requires agencies to (1) ensure that information systems security requirements, procedures, and practices are included in computer security awareness training material, (2) provide new employees an orientation outlining security responsibilities, and (3) provide training to employees on a regular basis.

RMA officials stated that all employees and contractors received mandatory annual IT security training in either January or February 2003 and that they believed that those needing specialized training also received it. However, the officials provided no documentation showing that the cited employees received the mandatory training during 2002, as required.

---

<sup>21</sup> Public Law 100-235, "Computer Security Act of 1987," Section 2.B(4).

<sup>22</sup> DR 3140-001, "USDA Information Systems Security Policy" (May 1996), Section 12.



- I. Performance Measures. RMA did not establish IT security performance goals and measurements. The Government Performance and Results Act of 1993 (GPRA) required RMA to formulate a performance strategy within its strategic plan to improve program integrity. RMA developed a performance strategy, but the strategy did not include IT security goals. For example, RMA should establish IT security goals to organizationally separate IT security operations from production operations and to accomplish effective system and application reviews, assessments, and certifications timely. The GPRA requires agencies to prepare annual performance plans and to establish performance goals. Also, the E-Government Act of December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
- J. Unauthorized Software. At least two users loaded unauthorized software on the RMA computers assigned to them. We reviewed the software present on 10 judgmentally selected RMA desktop computers and found unauthorized software applications on 2 of the 10 computers reviewed. We found an unauthorized streaming audio program on one computer and an unauthorized screensaver on the second computer. RMA has a process to “lock down” the computers from unauthorized software installation and inappropriate Internet use, but this control did not always operate effectively. As a result of ineffective controls for preventing users from loading and using unauthorized software, the vulnerability of RMA’s networks, systems, and data was increased.

OCIO’s Cyber Security Policy CS-010<sup>23</sup> states that USDA has a long established policy that does not condone or support employees’ use of Government computer or networks for unauthorized purposes. In addition, each agency should establish a system to monitor Internet usage using USDA equipment by employees and contractors to ensure they adhere to these policies.

We judgmentally selected 10 computers that were turned off and the users were not at the workstations. We determined if the

---

<sup>23</sup> OCIO Cyber Security Policy CS-010, “Interim Guidance on Peer to Peer (P2P) Software and Copyright Protection” (January 2002), Section 2.

software loaded onto the computer was properly licensed and authorized by RMA. The security staff removed the unauthorized software soon after we notified them of the two cases and reminded the employees that only RMA-approved software was allowed.

## **Recommendation No. 6**

Use this report to identify and include RMA IT organizational and security weaknesses in RMA's annual FMFIA report and in subsequent FMFIA reports until all material weaknesses have been corrected and IT operations substantially comply with applicable laws and regulations.

### **RMA Response.**

“RMA conditionally concurs. As discussed during the audit, not every weakness identified by OIG directly affects the Agency's financial systems. Weaknesses, recommendations and findings that directly relate to the health of these systems will be reported in the annual FMFIA report.”

### **OIG Position.**

RMA's written comments presented conditional concurrence with the recommendation, but the comments did not provide sufficient information to enable us to accept the management decision. To reach management decision, RMA needs to explain the process in detail that will be used to assess the agency's IT systems and the specific timeframes for implementation of the corrective actions.

## **Recommendation No. 7**

Develop, document, and implement an action plan with milestone dates for an overall strategy to address the weaknesses not cited in RMA's FMFIA reports.

### **RMA Response.**

“RMA concurs. The Administrator, in conjunction with the CIO, has already put into place an Audit Remediation Plan that includes every open item in the recent Security and Financial audits. Additionally, the Fiscal Operations and Systems Division and CFO management team are also incorporating related action items into the 5-Year FMS Plan as well as their own internal FMFIA Remediation Plan.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation, but the comments did not provide sufficient information to enable us to accept the management decision. To reach management decision, RMA needs to provide additional clarification showing the specific corrective actions included in the remediation plan and the specific timeframes for implementation of them.

### **Recommendation No. 8**

Prepare and submit quarterly status reports to OCIO until the cited weaknesses in FMFIA reviews and reporting, risk assessments, system certifications, security plans, contingency planning and disaster recovery, background investigations, incident response procedures, security training, performance measures, and unauthorized software are corrected.

### **RMA Response.**

"RMA concurs. RMA will provide the OCIO with quarterly summaries of activities completed and pending under the Audit Remediation Plan."

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation, but they did not provide sufficient information to enable us to accept management decision. To reach management decision, RMA needs to provide the specific timeframes for implementation of the quarterly summary submissions to OCIO.

---

### **Finding 4**

### **Improved Contract Administration is Needed to Assure Effective IT Security**

RMA contracted a national IT services provider under the General Services Administration (GSA) Millennium contract to perform key IT administrative, operational, and security duties and functions. Our reviews of controls over physical access to RMA IT equipment and logon accounts to RMA networks and systems disclosed that RMA did not administer the contract in accordance with applicable Federal requirements or the provisions of the contract because it directly supervised the day-to-day activities of the contractor employees. RMA did not establish effective controls to ensure that all necessary contract provisions were included and enforced and that applicable laws and

regulations were followed. Specifically, we found weaknesses in background investigations, documentation of services, and separation of duties. As a result, RMA put its own systems and IT hardware at greater risk of misuse, abuse, unauthorized access, disruption of service, and willful destruction by unscreened contract employees. Further, RMA similarly increased the risk to FSA IT assets by authorizing the unscreened contractor employees' access to a large Federal facility and to FSA IT equipment and information that was co-located with RMA equipment.

Background Investigations. RMA did not require background investigations for IT contractor employees and employees of associated subcontractors with access to RMA systems and hardware. Neither of the two contractor employees, working as a part of the IT security staff, or the other contract employees, working as system or network administrators, had been subjected to background investigations. RMA maintained approximately 40 LAN accounts for contractor employees, as well as 6 contractor accounts on production systems and 4 accounts for remote contractor access. In addition, RMA authorized physical access to IT equipment rooms in Kansas City, Missouri, for about 20 contractor employees. RMA officials stated that background investigations were not performed because (1) they were unnecessary since RMA systems had little sensitive information, (2) there was uncertainty over funding background investigations, and (3) the contract task order did not require them. However, we found that RMA systems maintain sensitive personal data on employees and program participants (such as social security numbers), as well as sensitive financial and program information. In addition, our review of the base GSA Millennium contract and applicable task orders disclosed that the contractor should have provided the background investigations as a part of the contract. Contractor employees are routinely authorized access to RMA systems, financial and program systems applications, and some contractors are authorized administrative or super-user access to systems that maintain sensitive data. We concluded that RMA and the contractor did not adhere to contract requirements or comply with applicable Federal laws and regulations.

Federal Regulations<sup>24</sup> and OMB Circular A-130<sup>25</sup> require that persons in positions of public trust and those who are authorized to bypass significant technical and operational security controls have periodic background investigations. DR 3140-001<sup>26</sup> requires personnel, including contractors, working in the ADP environment to have proper personnel security clearances.

---

<sup>24</sup> 5 CFR 731.106.

<sup>25</sup> OMB Circular A-130, Appendix III (November 2000), Subsection B.a.2b.2c.

<sup>26</sup> DR 3140-001, USDA Information Systems Security Policy, Subsection 10.d(5).

Section H.2.7, “Standards of Conduct and Restrictions,” of the Millennium contract and RMA task order states: “*The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel.*”

Section H.8, “Security Requirements,” states: “*The Government may require security clearances for performance of any TO<sup>27</sup> under this Contract ... Contractors are required to have background investigations for suitability if they occupy positions of trust (e.g., systems administrator) even if they do not have access to classified information.*” Although RMA modified this section in its task order, the modification had no impact on the requirement that contractors in positions of trust must be subjected to a background investigation. The level of trust RMA placed in the contractor employees should be measured against the level of system and hardware access granted to each contractor employee and the potential harm that could result from their physical access to a Federal facility and to co-located FSA IT hardware.

A GSA Contract Specialist agreed with the RMA official’s comment that the task order did not require background investigations for the contractors. However, when questioned, he could not explain the inconsistency between the requirement in the base contract and the revised RMA task order, which states: “*Paragraphs H.1 through H.20 of the contract awarded as a result of (the base contract) are applicable to this task order and are hereby incorporated by reference, except as modified below.*” The only modification to the security paragraph in RMA’s TO<sup>28</sup> was: “*This task order has no requirement for access to classified information.*” This modification did not state or imply that background investigations were no longer “incorporated by reference.” The GSA specialist added that RMA was working to revise the task order and to obtain background investigations for contractor employees. RMA officials stated that they needed to revise the contract to include a requirement for security background investigations.

Documentation of Security Services. Two employees of the contractor located at the Kansas City, Missouri, office were assigned key responsibilities for RMA’s IT system security. We attempted to identify details of security services or products expected or delivered by the contracted security specialists. The RMA Security Officer stated that the two contracted specialists reported directly to her for daily guidance and direction. RMA and the contractor did not prepare task orders or other documentation to describe the specific security services

---

<sup>27</sup> “TO” is an acronym for “task order.”

<sup>28</sup> Section H.8 of Modification PS08 of the RMA TO.

expected from the contractor employees or the details of the services provided by them. As a result, RMA and the contractor were not in compliance with contract provisions prohibiting direct supervision of contractors by Federal employees.

The specialists confirmed that the Security Officer supervised them and had no documentation of the work expected of them or the actual security services they provided. The contractor's project manager confirmed that all the security services provided were covered by the general IT service task order covering the work performed for RMA under the Millennium contract. The project manager also agreed "there was a problem" with the two contractor employees reporting directly to a Federal employee, the RMA Security Officer.

Section H.9.7, "Supervision of Contractor Personnel," of the Millennium contract task order states: *"The Contractor-supplied personnel are employees of the Contractor and under the administrative control and supervision of the Contractor. The Contractor, through its personnel, shall perform the tasks prescribed herein and in (task orders) issued hereunder. The Contractor shall select, supervise, and exercise control and direction over its employees under this Contract. The Contractor shall not supervise, direct, or control the activities of Government personnel or the employee of any other Contractor. The Government shall not exercise any supervision or control over the Contractor in the performance of contractual services under this Contract."*

Section H.9.8, "Specialized Disciplines," of the Millennium contract task order states: *"Specialized discipline requirements will be specified in individual Task Order Requests and, subsequently, individual Task Orders at time of issuance."*

Separation of Duties. Two employees of the contractor at the Kansas City, Missouri, complex worked directly in key IT security positions and on key production projects during the same period. Both employees were hired by the contractor as network specialists and were, subsequently, converted to security specialists. According to the contractor's records, the employees' primary responsibility was IT security. One security specialist (see block Cx2 in exhibit A) also worked as the contractor's lead person for configuration management, while the second security specialist (see block Cx1 in exhibit A) also worked as a network analyst. Contractors or employees who were charged with both key system security responsibilities and systems administration duties were in position to make decisions or take action that could result in intentional and unintentional errors, misuse, abuse, unauthorized access, disruption of service, and willful destruction. An

interview with the contractor's project manager disclosed that the project manager agreed there was a potential conflict in the security and production work assignments for these employees.

The "Preventive Management Security Controls" subsection of NIST SP 800-30 states: *"Implement personnel security controls, including separation of duties, least privileges, and user computer access registration and termination."*<sup>29</sup>

Exhibit A illustrates the cited conflicts with an RMA IT Security Officer (see block X1) and a secondary connection between the same security specialist and the RMA network administrator (see block X2 in exhibit A). Similarly, the security specialist shown as block Cx2 in the exhibit has a direct subordinate connection with RMA IT Security Officer (see block X1) and a secondary connection with the team leader of RMA's Configuration Management (see block A2e1). The contractor's project manager agreed this structure presented a potential conflict.

## **Recommendation No. 9**

Strengthen senior management oversight and periodically monitor and document the effectiveness of agencywide policies, procedures, and management controls to ensure that IT services contract provisions conform to all applicable laws and regulations and that contract provisions are enforced.

### **RMA Response.**

"RMA concurs. See Agency response to recommendations 3 and 5."

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation, but they did not provide sufficient information to enable us to accept management decision. To reach management decision, RMA needs to describe in detail the process that will be used to strengthen management oversight, monitoring, and documentation regarding the IT services contract provisions, and assess and provide the specific timeframes for implementation of the corrective actions.

## **Recommendation No. 10**

Require background investigations for all IT contractor employees and associated subcontractor employees, where applicable, and ensure they

---

<sup>29</sup> NIST SP 800-30 (October 2001), Subpart 4.4.2.1.

are satisfactorily completed before access to RMA systems, hardware, and facilities are authorized.

**RMA Response.**

“RMA concurs. The Agency is currently conducting background investigations on the most recent contractor hires. Background clearance for older contractor hires will be completed this FY. Federal employees will be investigated in the coming 24 months as budget allows. Language regarding the ongoing requirement for background checks has been submitted to GSA for incorporation within the Millennium contract.”

**OIG Position.**

RMA’s written comments presented concurrence with the recommendation and actions initiated to date, but the comments did not provide sufficient information to enable us to reach management decision. To reach management decision, RMA needs to provide the specific timeframes showing when the background check requirements will be incorporated within the Millennium contract.

**Recommendation No. 11**

Improve and document senior management oversight to ensure that Federal employees do not supervise the day-to-day activities of contracted security specialists and other IT contractor employees and to ensure adequate separation of duties and responsibilities assigned to individual contractor employees.

**RMA Response.**

“RMA conditionally concurs. RMA disagrees with some statements regarding direct supervision of contractors. Federal employees serve as leads, escalation points and technical representatives at some junctures in the contracting process. Typically, contractors have standing duties assigned to them by the contract company, such as ongoing monitoring and maintenance. RMA leads are not assigning work, however they provide the Agency's approval for work efforts to take place in effect authorizing work for billing.”

RMA will issue a document and training materials reminding employees of applicable regulations and proper conduct in relation to contracting. RMA will further document and regulate interaction between Agency officials and contracting staff and/or management to remove the perception of direct supervision of contractors.”



### **OIG Position.**

RMA's written comments presented concurrence with the recommendation and plans appropriate corrective actions. To reach management decision, RMA needs to provide an explanation of how the activities between agency personnel and contractors will be controlled and the specific timeframes for implementation of the proposed corrective actions.

### **Recommendation No. 12**

Prepare individual task orders and other supporting documentation, as needed, to describe the specific security services expected from contractor employees and to record the details of the services or deliverables to be provided by them.

### **RMA Response.**

"RMA concurs. RMA has already supplied the contracting firm and GSA with security tasking requirements in writing. These will be incorporated into the Millennium contract and have already been utilized to fill the current positions."

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation and plans for appropriate corrective actions. To reach management decision, RMA needs to provide the specific timeframes for incorporation of the tasking requirements into the Millennium contract.

---

### **Finding 5**

### **System Scans are Needed for Effective IT Security Management**

RMA has systems on its network that have potential serious security vulnerabilities. Significant weaknesses in RMA's system security administration were identified by our electronic system vulnerability scans on RMA's IT systems. The scans disclosed a large number of risk indicators that could be exploited, as well as system policy settings that did not provide for optimum security and uniformity throughout RMA. RMA acquired electronic scanning tools similar to those we applied; however, RMA did not properly conduct the scans that would allow it to identify the vulnerabilities within its network. Also, RMA did not fully develop a configuration management program to ensure that security patches and other software updates were routinely updated

on all systems and did not have adequate firewall protection. These conditions occurred because RMA did not develop or implement appropriate policies, procedures, and controls to effectively prevent, detect, and correct security vulnerabilities in its systems. Although RMA conducted limited system security scans on its own, RMA's officials were not aware that their systems and networks were vulnerable to cyber-related attacks that could jeopardize the integrity and confidentiality of RMA's systems. The scans were not conducted with sufficient frequency to identify recurring conditions after the initial weaknesses were found and corrected or to identify potentially harmful trends, errors, unauthorized access, or other notable events. As a result, these vulnerabilities, if left uncorrected, could jeopardize the security of the RMA network and its critical and sensitive financial and program data. RMA systems process, analyze, and support more than \$7 billion in financial and program data on an annual basis.

OMB Circular A-130<sup>30</sup> 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. In addition, Cyber Security Policy CS-007 states that vulnerability scans were to be performed on a monthly basis for all networks, systems, and servers by duly authorized users in accordance with established procedures. CS-007 also requires systems and network administrators to apply patches or fixes to networks and servers in a timely manner.

System vulnerability scans are effective tools for identifying and controlling a variety of security weaknesses. We used three commercially available software products to accomplish our scans. One was designed to identify over 1,100 different types of vulnerabilities associated with various operating systems that used Transmission Control Protocol/Internet Protocol (TCP/IP).<sup>31</sup> A second package tested system policy settings in network operating systems, and the third package searched for modems within a set or range of telephone numbers to identify potentially unsecured carrier lines. Details of the results of our scans and related analysis follow.

A. TCP/IP System Vulnerabilities. We conducted our vulnerability scans in WDC, and Kansas City, Missouri, and the following table lists the total vulnerabilities disclosed at each location.

---

<sup>30</sup> OMB Circular A-130, Appendix III (November 2000), Section B.

<sup>31</sup> TCP/IP is a series of protocols originally developed for use by the U.S. Military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms.

<b>Network Location</b>	<b>High Risk<sup>32</sup></b>	<b>Medium Risk</b>	<b>Low Risk</b>	<b>No. of Hosts</b>
Washington	5	27	56	37
Kansas City	116	158	476	170
Totals	121	185	532	207

The high and medium-risk vulnerabilities, if left uncorrected, could allow unauthorized users access to critical and sensitive RMA data. The large number of low-risk vulnerabilities identified also indicates that RMA needs to strengthen its system administration. Examples of the high-risk vulnerabilities identified during our scans include:

- A workstation was configured to allow anyone to sign on as the Administrator by using a blank password. This makes the system extremely vulnerable to unauthorized activity because the Administrator's account was used to maintain complete control over the system and could be used to perform any system function.
- Two e-mail access protocols contained vulnerabilities that could allow an attacker the ability to take complete administrative control of the systems.
- Three hosts were found with an accessible default account detected through a remote administration program because RMA maintained the original default software application settings for managing its computer networks. Original default settings are well known by attackers and can be used to easily obtain or change system information and to gain open connections with other systems. As a good security policy, these settings and related accounts should be removed, renamed, or protected with complex passwords.

RMA did not perform scans on a monthly basis for all networks, systems, and servers, as required by CS-007. RMA performed scans only twice during the 6-month period of April through September 2002. In May 2002, scans were conducted on desktop computers located in Kansas City, Missouri, and in various field offices. RMA did not have a documented process to record and verify corrections that were made. In August 2002, the vulnerability scans covered only machines with a specific

---

<sup>32</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 sensitive, but less significant, network data.

operating system. RMA network administrators stated that they were aware of the OCIO requirements, but RMA did not provide sufficient resources to perform scans on a monthly basis.

- B. Configuration Management. While RMA initiated a configuration management program by automating server configuration from a central location, more work was needed to fully implement the program. We conducted TCP/IP system vulnerability scans on Kansas City, Missouri, located RMA systems and identified 116 high vulnerabilities. Analysis of these vulnerabilities disclosed that 98 of the 116 high vulnerabilities (or about 84 percent) occurred because RMA's system administrators did not apply security patches and software updates that were available for their respective systems. We also determined that 56 of 90 machines were not configured with the correct security service pack. After we discussed the results of our scans, the RMA security staff advised us that they had applied all security-related patches and other software updates to their servers.

OCIO Cyber Security Policy CS-009, "Interim Guidance on USDA Configuration Management," defines configuration management as processes that are used to establish and maintain control of system/application software, and system and network physical infrastructure changes, ensuring that the system in operation was the correct system. NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states that, from a security point of view, configuration management provides assurance that the system in operation was the correct version (configuration) of the system.

Security-related programming flaws are generally discovered only after a large number of users begin to use the software and hackers and independent testers attempt to compromise it. After software programming flaws are discovered, software providers often release software updates to correct the flaws. These updates are often referred to as patches, hot fixes, or service packs. Today, more than ever, timely response to vulnerabilities is critical to maintain the operational availability, confidentiality, and integrity of IT systems.

A configuration management program ensures that all systems are routinely updated with recent security patches and other software updates. We believe a system configuration management program, which includes timely application of security-related patches and software updates, regularly scheduled and properly conducted vulnerability assessments, and timely remediation of the risks

discovered would substantially enhance the security of RMA's computer systems.

- C. Firewall Configuration. RMA did not have an internal firewall with an intrusion detection system in place at one location and one was not configured appropriately. RMA staff was not aware that they were not protected by the firewalls. As a result, no assurance was provided that external and internal intrusions would be properly addressed and reported.

According to NIST guidance,<sup>33</sup> the firewall environment should be configured carefully to minimize the complexity and management of the firewall, while at the same time, provide adequate protection for the organization's networks. A firewall policy is essential; firewalls are vulnerable to incorrect configurations, as well as system administrator's failure to apply needed security patches and other security enhancements.

Specifically, RMA's firewall configuration in Kansas City, Missouri, was maintained adequately; however, several firewall rules were in places that were either no longer needed or were not configured in the best interest of network security. Our system scans also disclosed that two high vulnerabilities and a medium vulnerability could be detected from outside the firewall.

At the time of our review, RMA's WDC, IT facilities did not include an internal firewall between the network and the Department's telecommunications backbone. Without firewall protection between RMA and the backbone, weaknesses in another USDA agency's network could have put RMA's IT resources at risk. Subsequent to our scans, FSA network personnel informed us that the RMA network was brought under the protection of the FSA firewall. Because we were unable to test the RMA firewall configuration settings during our audit, RMA should coordinate with FSA network administrators to review the WDC firewall configuration and placement to ensure FSA's firewall adequately safeguards the RMA network.

### **Recommendation No. 13**

Take immediate action to correct all high and medium-risk vulnerabilities identified by our vulnerability scans and conduct rescans to ensure that the vulnerabilities identified by us have actually been corrected. Require IT officials to track each vulnerability and certify

---

<sup>33</sup> NIST SP 800-41, "Guidelines on Firewall and Firewall Policy" (January 2002), Executive Summary.

that actions have been taken to remedy the problem for all vulnerabilities identified by our scans.

**RMA Response.**

“RMA conditionally concurs. Undisputed vulnerabilities will be corrected. Though the audit document indicates 306 medium and high-risk vulnerabilities, some vulnerabilities are disputed. For example, Novell users are not flagged as active when they dial-in. For a number of remote users, they will only be dial-in customers. These were picked up as "inactive accounts" by the scans. Novell cannot be reconfigured; it is a nuance of the environment.”

**OIG Position.**

RMA’s written comments presented conditional concurrence with the recommendation and show undisputed vulnerabilities will be corrected. For the disputed vulnerabilities, RMA should document the false positive vulnerabilities and retain this documentation for future scans. Also, Novell was not tested by the scans we used. To reach management decision, RMA will need to provide the specific timeframes for correction of the vulnerabilities.

**Recommendation No. 14**

Require IT officials to run vulnerability scans of the RMA’s entire network on a monthly basis to detect, track, and correct noted vulnerabilities. Establish a comprehensive plan that will assure effective testing of RMA’s network so that data is safeguarded and assess low-risk vulnerabilities to identify trends and initiate actions on those areas in the aggregate that could lead to more serious vulnerabilities.

**RMA Response.**

“RMA concurs. Scans were run, however insufficient man-hours were available to review results and document findings. While some reviews were conducted, they were not performed at regularly scheduled intervals and historical logs and findings were not retained for audit team review. As part of the Administrator's Audit Remediation Plan, the Agency is reviewing automated tools to support this process. Though automated tools will help facilitate this function, funding of additional manpower in FTE or contractors will be required.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation and provided an overview of anticipated corrective action. To reach management decision, RMA will need to provide the specific actions taken to correct identified system vulnerabilities until contemplated actions can be accomplished. The agency will need to provide the estimated timeframes for the correction action planned.

### **Recommendation No. 15**

Require IT officials to develop and follow a configuration management program for RMA's systems. Assure periodic tests are performed and track and correct items identified to ensure that the plan is in place and operating effectively. Codify descriptive management policies and procedures for these operations in RMA's directive system.

### **RMA Response.**

"RMA concurs, RMA has purchased and is implementing change/configuration management tools within both the business systems (Synergy) and the infrastructure (Magic Solutions) environment. RMA is also instituting uniform policies and procedures across the business systems and infrastructure for change/configuration that will include a Change Control Board as well as a fulltime Change/Configuration Management Officer."

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation and provided an overview of anticipated corrective action. To reach management decision, RMA will need to provide the specific actions taken or planned by the agency and the estimated timeframes for the correction actions.

### **Recommendation No. 16**

Develop and apply a policy to conduct a routine and timely review of RMA's firewall configuration and periodically verify the effectiveness of FSA firewall protection that RMA must rely upon.

### **RMA Response.**

"RMA concurs. The System Administration Chief and Security Team are currently implementing processes that include periodic reviews

supplemented by software that performs ongoing automated monitoring of firewall effectiveness.”

**OIG Position.**

RMA’s written comments presented concurrence with the recommendation and provided an overview of anticipated corrective action. To reach management decision, RMA will need to provide clarification of the specific actions taken by the agency including the frequency of the periodic reviews and the estimated timeframes for the correction actions.

**Recommendation No. 17**

Review the WDC, firewall configuration and placement to ensure the FSA firewall adequately protects the RMA network from intruders and periodically re-verify that the RMA network is adequately protected in the future.

**RMA Response.**

“RMA concurs. RMA is currently implementing the Cable Plant Project, which reconfigures RMA's access into and out of the USDA backbone within the DC office. It will allow the RMA to more strictly control access instead of deferring to Farm Service Agency access controls. Until such time as the WDC Migration is completed, the RMA will request that FSA Pacific and PIX firewalls be periodically tested for penetration vulnerabilities.”

**OIG Position.**

RMA’s written comments presented concurrence with the recommendation and provided an overview of anticipated corrective action. To reach management decision, RMA will need to provide the specifics on the schedule for periodically testing FSA firewalls and the estimated timeframe that the WDC migration will be completed for the correction actions.



## **Section 2. Security Program Management of Information Technology Resources**

---

Our review disclosed potentially serious vulnerabilities over access to RMA's networks and systems. RMA did not properly manage user and system administrator accounts or establish sufficient physical controls to ensure that only duly authorized personnel have access to RMA's IT resources. We attributed the access control weaknesses primarily to the agency's weak IT organizational structure that did not provide approved, agencywide policies and procedures for controlling access to RMA's networks and systems. Physical access control weaknesses may, in part, be caused by inadequate physical security services provided by FSA; however, RMA did not take proactive steps to ensure the adequacy of services provided or consistently apply existing controls to safeguard its IT resources. These deficiencies leave RMA's IT resources vulnerable to unauthorized access, potentially jeopardizing the integrity of RMA's mission critical systems and sensitive financial and program data.

---

### **Finding 6**

#### **Improvements are Needed in Network Operating System Policies and Procedures**

We found potentially serious weaknesses in RMA's management of password administration, system administrator accounts, generic or shared user accounts, and accounts with unknown users. Our assessment software (or scans) provides comprehensive and flexible-reporting capabilities of various access control settings, such as user account characteristics and password controls. We conducted the network operating settings scans in addition to the system security management scans described in Finding No. 5. Details of the results of these scans follow.

According to NIST SP 800-14, "Generally Accepted Principles for IT Security," identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. The following should be considered when using user ID's:

1. Unique Identification. An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise;
2. Correlate Actions to Users. The system should internally maintain the identity of all active users and be able to link actions to specific users;

3. Maintenance of User ID's. An organization should ensure that all user ID's belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users; and
4. Inactive User ID's. User ID's that were inactive on the system for a specific period of time (e.g., 3 months) should be disabled.

We did not find RMA senior management approved policies or procedures on password settings, establishing and maintaining administrator accounts, or prohibiting the use of shared accounts.

Password Administration. RMA networks generally required users to change their passwords every 90 days; however, 60 days is the required timeframe. Also, some accounts were set up with passwords that never expired. Our scans found that 333 of 2,357 RMA user accounts (about 14 percent) had passwords that did not automatically expire within the 90-day limit. We also found user accounts that were configured with unlimited grace logins, which allowed the employee to retain the same password for an indefinite period because the system would not require the user to change the password.

According to NIST SP 800-14, "Generally Accepted Principles for IT Security" (September 1996), passwords should be changed periodically. OCIO Cyber Security Policy CS-013 (March 2002) requires passwords for all systems, applications, or processes and states that the passwords should be changed every 60 days for general users. Passwords issued to system administrators, system managers, and software engineers, or those that are used for dial-in access are to be changed every 30 - 45 days.

RMA Kansas City, Missouri, Security Staff stated they were aware of the password change requirements but, due to user complaints, they set the password change requirement at 90 days. To compensate for the variation from Departmental standards, users are required to select passwords with a combination of alpha, numeric, and special characters. However, we believe the use of 8-character passwords does not adequately compensate for the potential damage of compromised passwords left unchanged.

Administrator Accounts. While the conditions noted above identify weaknesses in the networks we reviewed, many of these conditions were also noted in accounts configured to provide the user overall access to the system or administrator access. The system administrator is the most trusted position on a system. The administrator has complete control of the system and has unrestricted access to any

information on that system, including sensitive information. The vulnerabilities of RMA's systems were magnified due to the following examples of conditions identified by our scans:

- 68 administrator accounts, or accounts that belonged to users with super access, were configured with passwords that did not expire;
- 29 administrator-equivalent accounts were also generic or shared accounts, permitting more than one person to perform administrator operations on the system without accountability for any individual user;
- administrative-equivalent users from the FSA network had access to RMA's WDC, network servers, even though their job responsibilities were limited to FSA;
- the password for the desktop computer used by RMA's lead desktop administrator was stored in readable text, rather than encrypted. The computer was configured with a default password and automatically logged in the default user when the machine was turned on. Anyone who started the computer was automatically logged on as the system administrator, with all the access rights and privileges generally configured for administrator accounts; and
- the network administrator for the new Kansas City, Missouri, network had insufficient rights to access information about three machines connected to the network. The administrator identified this problem on one server after our scan and corrected the problem. The second machine was later identified as a desktop, and the third machine could not be located in RMA's inventory.

Generic or Shared User Accounts. Our scans identified 312 generic, or shared, user accounts on RMA systems and networks. Generic or shared accounts are user accounts that are accessed by more than one person. These accounts make it impossible for system administrators to track the actions of users in the event that inappropriate or malicious action was taken.

OCIO Cyber Security Policy CS-013 (March 2002) requires that each access, whether a user account or process, be identified to a specific individual and may not be shared with a second or multiple parties. According to the policy, if a process cannot be specifically tied to an individual, then the password lifetime should be limited to the period of the session.

Unknown User Accounts. Our scan discovered an “Unknown User” account on a Kansas City, Missouri, LAN. An unknown user is a person or entity who has obtained a user ID and password without authorization. The account may belong to an RMA employee, a contractor, or an unauthorized person with no legitimate business on RMA systems. Responsible RMA managers could not provide an explanation for this weakness after we brought it to their attention or during subsequent discussions.

Based on the results of our review, RMA’s Kansas City, Missouri, Security Staff reset all accounts having administrator equivalency to enforce RMA’s password policy settings. In addition, the RMA Security Staff revoked administrator access on two generic accounts. A third generic account was renamed and the password reset, with only the security team informed of the password. According to the Security Staff, the password will be given out on a case-by-case basis to perform administrative functions that cannot be completed using a regular administrator account. While knowledge of the password for this account has been removed from all administrative users, we believe this generic account should also be removed from the network. If a user needs temporary administrative access, the Security Staff should temporarily provide administrative access to the user’s account and remove that access when the task is completed and administrative access is no longer needed.

## **Recommendation No. 18**

Correct the cited network vulnerabilities disclosed in this finding. Also, develop and implement formal written policies establishing minimum security setting and user configuration guidelines for RMA networks, periodically reassessing those settings and user configurations, and establishing a process to ensure the correction of those settings and configurations found to be misapplied.

### **RMA Response.**

“RMA conditionally concurs. Vulnerabilities not identified and disputed in this document will be corrected. RMA disputes the SNMP<sup>34</sup> vulnerabilities cited. RMA regularly used this protocol for Internal Network Management to manage internal switches, routers, and other network devices. We block all other access into our network (With the exception of OCIO Read Only permissions) for SNMP. Written policies and procedures to address the deficiencies are currently being drafted. Ongoing monitoring processes will be instituted upon approval of the policy.”

---

<sup>34</sup> “SNMP” is an acronym for “Simple Network Management Protocol.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation and provided an overview of anticipated corrective action. To reach management decision, RMA will need to provide the specifics on the schedule for periodically testing FSA firewalls and the estimated timeframe that the WDC migration will be completed for the correction actions.

### **Recommendation No. 19**

Identify the user of the "Unknown User" account with unrestricted access to RMA's servers. Depending on the identification of the user, either configure the system to maintain the identity of that user internally or file an incident report with OCIO regarding the security weaknesses of the systems that allowed the condition to exist.

### **RMA Response.**

RMA does not concur. Auditors were briefed on the fact that the "unknown account" in the Windows 2000 domain (OP) was the enterprise administrator account in the "placeholder" (RM) domain. The OP domain could not resolve the account because it does not exist in the OP domain. The account has full privileges in the OP domain because of the nature of Windows 2000 Active Directory.

### **OIG Position.**

During the course of our review, RMA offered three possible explanations for the "unknown account" but was unable to supply documentation to support the explanation. We are able to accept management decision on this recommendation because RMA has now confirmed that the account has full privileges in the OP domain because of the nature of Windows 2000 Active Directory. For final action, RMA needs to provide the OCIO with documentation showing the account now has full privileges in the OP domain.

---

**Finding 7****Stronger Controls are Needed to Restrict Access to RMA Systems and Networks**

RMA did not establish formal or effective controls to properly manage or oversee the administration of RMA's user accounts on RMA, National Information Technology Center (NITC), and the Office of Chief Financial Officer's (OCFO) National Finance Center (NFC) systems. We found no RMA written policies and procedures on administering the agency's user accounts on its internal or Departmental IT systems. We identified significant and recurring weaknesses in three areas of account administration, including retention and maintenance of user accounts, user access rights and privileges, and administrator privileges. RMA did not properly assign user accounts and access privileges to restrict access to data and files or adequately evaluate users to ascertain their continuing need for system access, maintain a current list of all users by system, and timely remove access for separated employees and contractors. These vulnerabilities, if left uncorrected, could jeopardize the security of RMA's network and its critical and sensitive financial and program data.

Effective administration of users' computer access is essential to maintaining system security and ensuring access is limited to authorized users. User account management focuses on identification, authentication, and access authorizations. The process of auditing and periodically verifying the legitimacy of current accounts and access authorizations augments administration activities. It is important to realize that access and authorization administration is a continuing process. Our audit did not detect unauthorized access instances but noted the following potentially serious weaknesses.

- A. Improprieties in User Accounts. We reviewed the management and control of RMA's user accounts on RMA, OCFO's NFC, and NITC systems and identified (1) 16 active accounts for former employees and contractors, (2) 745 dormant accounts on a major IT platform, (3) 371 shared or generic accounts that could not be associated with an active RMA employee or contractor, (4) 259 accounts that should be deactivated or deleted, and (5) 89 accounts with questionable dial-in access to RMA systems.

DM 3140-1.6<sup>35</sup> requires agencies to use individual user ID's and passwords to control access to systems processing financial, market-related, personnel, or other sensitive data. Further,

---

<sup>35</sup> DM 3140-1.6, "Management ADP Security (Part 6 of 8)" (March 1992), Section 4a.

Section 6c, requires staff to remove employee user accounts and passwords when the employee is no longer employed with RMA. OMB Circular A-130<sup>36</sup> lists individual accountability as a primary mechanism for personnel security. It recognizes that accountability is accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. Cyber Security Policy CS-013<sup>37</sup> explains that user ID's should be identified with an individual user and not shared. If the user ID cannot be tied to an individual user and not shared, the password should only be issued for a particular session. DM 3140-1.3<sup>38</sup> also explains that agencies should maintain accounting and access logs sufficient to permit RMA to reconstruct events, should a security violation occur.

Former Employee and Contractor Accounts. RMA's process for ensuring the prompt termination of system access for separated employees and contractors did not effectively terminate access. A Human Resources Specialist explained to us that employees were responsible for requesting the Security Officer to terminate their access from RMA systems as a part of the agency's separation process. We identified 16 separated employees and contractors who retained open access accounts for RMA systems after their employment ended. This process provides no assurance that access to mission-critical systems and applications is terminated when employees leave RMA service. As a result, critical RMA data are vulnerable to destruction or revision by disgruntled former employees, and the agency is vulnerable to loss or disruption of IT services.

Dormant Accounts. RMA maintained 745 active accounts on a major system for users that did not log on to the system after the accounts were established. The system administrator did not remove user accounts from the system after they became inactive because he did not have an automated process to do so. Dormant accounts can be identified by knowledgeable hackers, contractors, and employees and used for any number of inappropriate system activities with low risk for detection. The large number of dormant accounts can be an indicator that system administrators do not adequately monitor account activities through system reports or take aggressive steps to restrict access to the system by outside hackers and other unauthorized users. NIST principles and practices provide a baseline that organizations can use to establish and review their IT programs. Specifically, user accounts should

---

<sup>36</sup> OMB Circular A-130, Appendix III (November 2000), Subsection A.3b.2c.

<sup>37</sup> OCIO Cyber Security Policy CS-013, "C2 Controlled Access Protection" (March 2002), Section 2.

<sup>38</sup> DM 3140-1.3, "Management ADP Security (Part 3 of 8)" (March 1992), Section 16e.

be disabled after they are inactive on the system for 3 months or other specified period.

Generic or Shared Accounts. Our scans identified a total of 371 shared or generic user accounts on RMA systems. Generic user accounts are not devoted to a particular person and may be accessed by any number of people. Generic/shared accounts prevent accountability to management for improper system activities and inappropriate access to critical systems and sensitive data. The RMA Security Officer identified the specific purpose for many of the questioned accounts, such as system utilities, training, and user accounts. However, she could not identify the purpose for the accounts or associate a specific user for 59 generic accounts authorized access to the Kansas City, Missouri, LAN.

Unneeded User Accounts. We compared listings of RMA users on RMA, NITC, and OCFO's NFC systems to a list of current RMA employees and found a total of 259 active accounts that we could not associate with an RMA employee or contractor. We discussed this condition with the Security Officer and RMA deactivated 151 of the 259 accounts. The 108 remaining accounts included:

- 44 unused accounts named "NoName" with no identifiable user. The accounts were originally opened for existing employees, but due to non-use or security requests, OCFO's NFC changed the account names and moved them into a reserve pool instead of deleting or deactivating them;
- 48 accounts that included two sub-accounts, one of which could not be accessed by RMA employees. These accounts should also be deactivated. The RMA Security Officer believed these were training accounts that NFC set up for RMA employees and were out of RMA control; and
- 16 unused accounts that remained active after the users no longer worked for RMA or its contractors.

Dial-In Access. Our scans also identified limited dial-in access for 347 Kansas City accounts. Further review of these accounts disclosed 89 questionable dial-in authorizations. We found:

- 61 dial-in generic accounts for which the Security Officer could not provide either a specific user's name or the reason that dial-in access to RMA systems was needed;



- 13 dial-in accounts were attributed to a specific person, but the Security Officer could not identify the employer of the person or provide the reason the person needed dial-in access to RMA systems;
- 12 dial-in accounts for FSA employees for which the Security Officer could not provide justification or a need for dial-in access to RMA systems; and
- 3 dial-in accounts remained active for separated employees or contractors.

B. User Access Rights and Privileges. RMA did not establish adequate controls to ensure that employees and contractors were authorized appropriate user rights and privileges to accomplish their duties and responsibilities without authorizing unneeded capabilities (read, write, execute) to view or change system or application software and data. This occurred because RMA did not maintain an inventory or central file of the access rights and privileges authorized for each user account to ensure that approved authorization did not exceed the scope of each person's duties and responsibilities. RMA managers did not periodically review user accounts to verify that users and their account profiles were appropriate.

NIST SP 800-12<sup>39</sup> states that, from time to time, it is necessary to review user account management on a system. For example, a good practice is for application managers (and the data owner, if different) to review all access levels of all application users every month and sign a formal access approval list, which will provide a written record of the approvals. NIST SP 800-12<sup>40</sup> also states the access request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile.

NIST 800-12<sup>41</sup> states that while it may initially appear that systems personnel should conduct reviews, such reviews are not usually fully effective. System personnel *can* verify that users only have those accesses authorized by their managers. However, because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.

---

<sup>39</sup> NIST SP 800-12 (October 1995), Section 10.2.2.

<sup>40</sup> NIST SP 800-12, Section 10.2.1.

<sup>41</sup> NIST SP 800-12, Section 10.2.2.

The RMA Security Officer stated that she did not maintain a file to track user rights and privileges; system administrators monitored access for their respective systems through application security liaison representatives. We also found that program and security managers did not review changes to the security profiles, independent of the security staff, to ensure access authorizations were consistent with employee responsibilities. The reviews were delegated to security liaison representatives, who may not be aware of the scope of each user's responsibilities. As a result, RMA did not ensure that user access and capabilities were limited to only those applications, databases, and functions that were necessary to perform their individual duties and responsibilities.

We reviewed system user ID files and our automated scans and determined that RMA maintained about 1,600 active user accounts for Kansas City systems. These accounts were assigned to employees, contractor employees, system administration, training, and system hardware and accessories. The Security Officer stated that she required an authorization form for all user accounts, including those for system hardware and accessories. However, due to inadequate record management, we could not establish the total number of accounts with a valid access authorization form on file.

We reviewed the access authorization forms for 447 accounts and found that the access rights approved for each employee and contractor were not always listed on the forms. The Security Officer stated that she did not maintain a record of all the rights and privileges assigned to each account, so she had no way of knowing if all users were authorized the rights and privileges appropriate for their current duties and responsibilities and no others. The Security Officer also explained that she maintained authorization forms for only 2 years, even though access rights and privileges of the employee or contract employee may change over time. We found multiple authorization forms for some accounts and that forms for other accounts were discarded before a revised form was submitted, leaving no central record of the rights and privileges assigned to a particular user for all systems and applications. As a result, the Security Officer did not maintain sufficient account information about each user to assure compliance with the "least privileges" concept outlined in NIST SP 800-12.

RMA officials believed that program managers' reviews of approved access authorizations would not be meaningful. However, data managers and organizations should periodically

review user account profiles to assure that all access authorizations to system data and files are appropriate.

- C. Administrator Access Privileges. RMA did not limit access to system administrator accounts (or login ID's) on two major IT systems located in Kansas City, Missouri. On one system, at least 112 people were authorized access to a file that listed passwords for other system administrator accounts. Administrator accounts provide authorized users the highest level of system access, enabling them to manage all aspects of the system, including any mainframes, servers, workstations, printers, etc., that were a part of that system. Multiple users under a single logon ID prevent identification of the person or persons who are responsible for any action taken on the system.

Both OMB Circular A-130<sup>42</sup> and NIST SP 800-12<sup>43</sup> stress the need for agencies to implement the “least privilege” concept, granting users only those accesses required to perform their duties. The application of this principle limits the damage resulting from accidents, errors, or unauthorized use of system resources. According to NIST 800-12,<sup>44</sup> access control often requires that the system be able to identify and differentiate among users. User accountability requires the linking of activities on a computer system to specific individuals and, therefore, requires the system to identify users.

The following examples illustrate conditions where there was no individual accountability for system operations when as many as 112 employees and contractors were permitted unlimited administrator privileges for the system. For the first case, our automated system security scans identified 112 user accounts on System A with access to a password protected file that contained generic account names and passwords for administrator accounts on the system. Generic accounts are shared accounts, providing system access for multiple users. RMA officials acknowledged there was little need for 112 individuals to have access to the password file and stated that they were not aware that all of the people listed were authorized access. When we notified RMA of the vulnerability, the responsible system administrator restricted access to the file.

For the second case, at least five people shared one generic administrator account (or login ID) on System B. The system's

---

<sup>42</sup> OMB Circular A-130, Appendix III (November 2000), Subsection B.a.2.c.

<sup>43</sup> NIST SP 800-12 (October 1995), Section 10.1.1.

<sup>44</sup> NIST SP 800-12, Introduction to Chapter 16.

administrator stated that he verbally informed the other four users when the account's password was changed so that all five users could use the account. This means that all five individuals had full access to read, write, or execute operations on all data, applications, and system administrative functions without identifying the specific person responsible for any particular occurrence. RMA officials were unaware of this generic administrator account.

## **Recommendation No. 20**

Develop internal written policies and procedures that establish effective access controls for RMA-controlled users to follow in using RMA, NITC, and NFC systems in accordance with applicable Federal guidance and DR requirements. Conduct periodic reviews to ensure RMA user compliance with the policies and procedures implemented.

### **RMA Response.**

“RMA conditionally concurs. RMA will develop the policies and procedures discussed in Recommendation 20, however, RMA still disputes findings related to NFC as their systems are outside RMA control.”

### **OIG Position.**

RMA's written comments presented conditional concurrence with the recommendation and provided an overview of anticipated corrective action but disagrees that NFC related passwords are under RMA control. OIG believes that agencies maintain responsibilities for accounts “belonging” to them on NFC systems. To enable us to accept management decision, RMA will need to provide the specifics on the policies and procedures to be developed and periodic reviews to be performed as well as timeframes for completing the planned actions.

## **Recommendation No. 21**

Evaluate the user accounts cited as dormant, lapsed, or unnecessary and deactivate those without confirmed justification for the remaining active accounts. Also, develop and implement a workable methodology to periodically review the activity of all user accounts to promptly identify and remove unnecessary accounts.

### **RMA Response.**

“RMA concurs. Problem accounts identified in the course of the audit have already been researched and removed as appropriate. The Security Team is implementing an automated process combining several tools such as Magic and Tripwire to further improve tracking and removal of inactive accounts.”

### **OIG Position.**

RMA’s written comments presented concurrence with the recommendation and provided that problem accounts identified have already been researched and removed. To enable us to accept management decision, RMA will need to provide the methodology utilized and specific implementation schedule for Magic and Tripwire, as well as personnel responsible for tracking and removal of inactive accounts.

## **Recommendation No. 22**

Develop and implement an effective process to promptly identify and terminate user accounts and system access to all RMA systems when employees and contractors are separated from RMA employment and/or service, as applicable. This process should entail RMA management and/or supervisors being accountable for notifying the security officer of employees or contractors being separated.

### **RMA Response.**

“RMA concurs. The agency is taking measures to improve tracking of inactive accounts and reporting of transfers, terminations and other events that trigger a change in security status for employees and/or contractors.”

### **OIG Position.**

RMA’s written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specific measures taken or planned and the estimated timeframes for completion of the corrective action.

## **Recommendation No. 23**

Terminate all generic and shared accounts and establish a policy to prohibit their use in the future. Implement a process to periodically

review accounts to verify that only one person is accountable for all access and activities performed with or through each user account.

**RMA Response.**

“RMA does not concur. Auditor analysis regarding "Generic or Shared Accounts" is incorrect. RMA technicians explained the difference between a generic account, a shared account, and a service account as defined by RMA, Microsoft, Sun, and other IT companies. A service account is used by the system to run applications such as email or databases. By nature, these accounts will have passwords that do not expire because the account is not "owned" by any individual. No "person" knows or holds the password; therefore, an administrator has to change the password. When new passwords are needed, they are generated by the system, making them superior to passwords created by a human. It is RMA policy to obscure the names of these accounts by naming them something other than system specific or service specific names (e.g., administrator or SQLAdmin).”

**OIG Position.**

OIG agrees that system service accounts are not the same as generic or shared accounts. The accounts OIG is concerned about were not service accounts but were accounts such as “backupguy”, “Guest RMA”, and “RMA Webteam.” To enable us to accept management decision, RMA will need to provide the specific measures taken or planned to terminate the accounts and provide policy to prohibit their use in the future, as well as the estimated timeframes for completion of the corrective action.

**Recommendation No. 24**

Immediately remove dial-in access for generic accounts and unknown or unidentified users. Also, establish effective controls, such as periodic reviews, to ensure dial-in access is needed, secured, approved, maintained, and periodically monitored to ensure only one user per account. Terminate authorization for dial-in access promptly after the need for access has ended.

**RMA Response.**

“RMA conditionally concurs. Periodic reviews of all accounts and their access level will be instituted as will a more reliable account termination processes. There is dispute regarding generic accounts and unknown and unidentified users. Auditors were briefed on the fact that the "unknown account" in the Windows 2000 domain (OP) was the enterprise administrator account in the "placeholder" (RM) domain.

The OP domain could not resolve the account because it does not exist in the OP domain. The account has full privileges in the OP domain because of the nature of Windows 2000 Active Directory. The document overstates the kind and number of weaknesses related to password and ID administration. This is due, in part, to a difference in interpretation between RMA and OIG technicians including a dismissal of the nuances between operating systems. For example, OIG determined excessive unused accounts. Even after discussion about nuances of Novell and the fact that Novell does not log remote users as active nor can you make Novell log remote users as active this was still reported as a problem condition.”

#### **OIG Position.**

RMA’s written comments presented conditional concurrence with the recommendation and shows that periodic reviews of all accounts and their access level will be instituted, as will a more reliable account termination processes. To enable us to accept management decision, RMA will need to provide the specific measures taken or planned and the estimated timeframes for completion of the corrective action.

### **Recommendation No. 25**

Establish controls to ensure that user rights and privileges are limited to those necessary for each user to fulfill his/her duties and responsibilities. These controls should include a central inventory file showing the rights and privileges authorized for each user on each system that is maintained and requirements that the file be periodically reviewed by RMA managers, supervisors, and the Security Officer to ensure user rights and privileges are current.

#### **RMA Response.**

“RMA concurs. To remedy this problem, RMA will be utilizing a segregated database within the Magic tool. Security levels will be tracked and matched against system components. Unauthorized changes will be identified via Tripwire and reported to the appropriate security and system administration personnel. The Administrator has approved a full-blown reassessment of access for every employee and contractor. This process will establish and record the new baseline in the automated system.”

#### **OIG Position.**

RMA’s written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA

will need to provide the estimated timeframes for completion of the corrective actions to be taken, including implementation and utilization of the segregated database within the Magic tool; security level tracking and matching against system components; identification of unauthorized changes via Tripwire; reports to the appropriate security and system administration personnel; and the full-blown reassessment of access for every employee and contractor.

---

**Finding 8****Stronger Physical Security is Necessary for Shared IT System Hardware and Facilities**

RMA did not ensure that adequate physical security components were in place to safeguard major computer systems and hardware. We found that RMA did not limit physical access to RMA's systems and hardware to only those with a need for access, did not ensure that security cages for equipment were kept locked to restrict access, and did not maintain a log to track the location and custody of critical system tapes. Although these weaknesses may, in part, be attributed to inadequate physical security services provided by FSA, RMA did not take steps to ensure the adequacy of the services provided or monitor activities to ensure that security cages were locked and that system tapes were properly safeguarded. As a result, RMA IT equipment and critical information were vulnerable to inadvertent and/or willful damage or destruction, loss of service, and theft.

OCIO Interim Guidance on Physical Security in USDA Information Technology Restricted Space, CS-005,<sup>45</sup> chapter 2, part I, paragraph 4(a), states: *"Only USDA personnel and authorized contractors having an ongoing recurring business need will be given unescorted access to the IT Restricted Space; review of this access should be done quarterly to minimize the number of people granted access."* Paragraph 4(b) states: *"Any employee or contractor who no longer has a business need to enter Restricted Space will immediately be removed from the access control system."* DM 3140-1.2, part 2 of the Department's Management ADP Security Manual, paragraph 15, requires all Departmental ADP installations to maintain logs to record the location of files and equipment, which have been removed from the ADP facility. We interpret this regulation to include removal of systems tapes from tape libraries.

Access to Computer Rooms. RMA was co-located with FSA in a USDA building in Kansas City, Missouri. In addition to GSA

---

<sup>45</sup> OCIO Cyber Security Policy CS-005, "Interim Guidance on Physical Security in USDA Information Technology Restricted Space" (November 2001), Chapter 2, Part I, Paragraph 4(a).



contracted security guards, FSA augments the physical security of the building by administering a magnetic access system. The system used individually programmed key cards (issued to selected employees, contractors, and vendors) to control unescorted access to secured computer equipment areas. These individuals must use their key card to gain entry to the building, as well as to enter the computer rooms. We found that 215 RMA and FSA employees, contractors, and vendors were authorized access to one or both of two computer equipment rooms. The following table shows the number of people authorized access to the main computer room and an auxiliary room used to maintain RMA servers. Both of these rooms were shared by RMA and FSA.

ACCESS AUTHORIZED FOR:	TOTAL	MAIN COMPUTER ROOM ONLY	AUXILIARY SERVER ROOM ONLY	BOTH ROOMS
Security Guards	18	-	-	18
FSA Employees	116	76	5	35
RMA Employees	10	5	-	5
Contractors/Vendors	70	34	7	29
Others (Visitor)	1	1	-	-
Total	215	116	12	87

We did not evaluate the need for access by all 215 people; however, it is unlikely that all 215 people had “an ongoing recurring business need” for unescorted access. Although an FSA official stated that he periodically requested FSA and RMA managers to review the lists of authorized employees and contractors, neither agency had a control in place to ensure the authorization lists were reviewed quarterly. The vulnerability of RMA’s and FSA’s equipment was compounded by the fact that RMA did not obtain background investigations for its contractor employees. Based on RMA and FSA records, at least 64 of the 70 contractor employees were contracted by RMA. RMA authorized unescorted access to critical RMA and FSA systems equipment for 22 of the 64 contractor employees, and none of them were subjected to a background investigation.

RMA’s IT hardware was physically located at one end of the main computer room, segregated, but not isolated, from FSA’s equipment in the remaining space. Also, one of two entries into the room was located at the end of the room adjacent to the space where the RMA equipment was located. As a result, RMA IT resources were vulnerable to unauthorized access by FSA employees, contractors, and vendors or vice versa. Security could be improved with the installation of a barrier, such as a heavy-duty metal screen, to deny unnecessary

access to RMA equipment without inhibiting ventilation and cooling. A second option would be to improve video surveillance of the rooms. We observed a camera installed in the RMA end of the main computer room, but the camera provided limited surveillance, due to its restricted capabilities. The camera operated only between 6:00 p.m. and 6:00 a.m.; it recorded only a small section of the RMA equipment room; it provided low-quality pictures that, according to a contractor employee, were comparable to those produced by residential “web cams;” and, finally, images from the video camera were not transmitted to the security room for monitoring by security personnel. Instead, still images from the camera were transmitted to an e-mail account that, according to one RMA contractor employee, was reviewed daily by a contractor employee.

Open Security Cages. During two site visits, we observed keys left in the locks of security cages used to secure RMA servers. Anyone with access to the computer rooms also had access to the unlocked servers. We also noted that not all RMA equipment was maintained in security cages. For example, a remote access server, located in the main equipment room and used for a critical business function, was maintained on an open shelf without a security cage.

System Tape Library. RMA also maintains a tape library in the main computer room. The library includes several locked cabinets and each database administrator maintained keys to the library cabinets. We reviewed the library and found that the database administrator for a critical system could not account for all the tapes that should have been stored in the library. The tapes could not be located during our visit, even though only five RMA employees were authorized access to them. We found that none of the database administrators maintained logs to record who and when tapes were removed from or returned to the library. This occurred, in part, because RMA did not prescribe procedures requiring that checkout logs be maintained for system libraries. Such logs help to ensure that tapes are accessed only by authorized personnel and are returned promptly.

## **Recommendation No. 26**

Restrict physical access to RMA IT system hardware to only RMA employees and contractors with an ongoing recurring business need for unescorted access to restricted IT spaces. Conduct periodic monitoring of personnel granted access to the cited computer room and ensure only authorized personnel are granted access.

### **RMA Response.**

“RMA concurs. RMA is working with FSA ASD<sup>46</sup> to remedy this deficiency. Separation of the RMA/FSA facilities is contingent on cost analysis by FSA ASD to expand computer room space and RMA's ability to fund its share of the expansion.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specific measures taken or planned and the estimated timeframes for completion of the corrective action. This includes contingency measures RMA plans to implement to restrict access in the event the proposed funding is not available.

### **Recommendation No. 27**

Establish a procedure requiring authorized database personnel to log the removal and return of system tapes to and from system libraries. Also, require periodic reviews to ensure that the procedure is implemented and logs are properly maintained.

### **RMA Response.**

“RMA conditionally concurs. RMA has taken steps to improve backup and recovery processes including the check-in, check-out, logging and storage of tapes and other media. These functions are outlined in SAB<sup>47</sup> operating procedures and have been vested in SAB Operators, however these individuals are not "database personnel" per se.

### **OIG Position.**

RMA's written comments presented conditional concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specific measures taken or planned on periodic reviews to ensure the procedure is implemented and logs properly maintained and the estimated timeframes for completion of the corrective action.

### **Recommendation No. 28**

Establish a formal policy and conduct periodic reviews to ensure that equipment security cages are locked when authorized personnel do not

---

<sup>46</sup> “ASD” is an acronym for “Administrative Services Division.”

<sup>47</sup> “SAB” is an acronym for “Systems Administration Branch”.

require immediate access and keys are controlled to ensure they are always recovered before personnel are separated from employment or from needing access.

**RMA Response.**

“RMA concurs. RMA will institute a spot-check procedure to monitor that security cages are properly locked and that keys are secured and only accessible to authorized personnel. This work has been and is ongoing. In February of 2004, the Network Group locked all Server racks, and stored keys in safe locations. During the March Maintenance Weekend, the primary RMA Router Rack was upgraded to a front/back locking rack with keys stored in safe and secure locations. The remaining racks will be converted on an ongoing basis in the coming months. In an effort to more strictly control access a key box is being procured; security staff will log in and check out keys to administrators.”

**OIG Position.**

RMA’s written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the estimated timeframes for completion of the corrective actions, including procuring the key box and converting the remaining racks.

### **Section 3. Application Controls and Tests**

---

Management controls over changes to application programs are critical in preventing unauthorized software programs or modifications to programs from being implemented. Key aspects of controls over application changes include ensuring that (1) software changes are properly authorized by the managers responsible for the program or operations that the application supports, and (2) new and modified software programs are sufficiently tested and approved before they are implemented. We found that RMA's application development and production operations did not adhere to the Department's SDLC methodology or sufficiently control software changes to the application, as required. Our review of one of RMA's three mission-critical system applications also disclosed that RMA did not apply appropriate management controls during development, testing, and maintenance of the application. This occurred, in part, because RMA did not prescribe agencywide policies, procedures, or controls to implement the applicable DR provisions or to provide appropriate criteria to assure that employees and contractors always applied the appropriate regulations and methodology, when required. As a result, inherent weaknesses in the RMA IT applications may remain undetected and uncorrected.

---

#### **Finding 9**

#### **Implementation of the System Development Lifecycle Methodology Would Improve Security and Performance**

RMA did not apply the required phases of the SDLC methodology to the development and implementation of a mission-critical system application for the 2003 insurance year. The responsible manager stated that the formalized SDLC process was not applied to this application because the modifications were made to an existing application used for the preceding reinsurance year, and the software programming changes were minor. Accordingly, we found the application was brought into production without the benefit of required pre-production tests and imbedded data validation routines. As a result, the vulnerability of Application E to errors and misapplication was increased.

We judgmentally selected Application E for our review, based on its status as a mission-critical application and due to the relationship of the application to RMA's financial reporting for the reinsured companies that deliver Federal crop insurance programs. DM 3200-001 states that a major application is one that directly affects the Department's ability

to meet a critical Departmental, national, or international mission. RMA identified Application E as a mission-critical system.

The SDLC methodology provides detailed guidance for the three phases of application lifecycle to properly manage major application system development projects in the USDA. In general, the SDLC provides specific guidance for the Initiation Phase, the Development Phase, and the Operations and Maintenance Phase. The Initiation Phase provides guidance for the process and analysis activities necessary to investigate the need for an application system development project. The Development Phase presents detailed guidance for developing an application in four stages, including the system analysis stage, the system design stage, the system construction and acquisition stage, and the user acceptance stage. The Operations and Maintenance Phase provides guidance for implementation and maintenance of the application.

RMA officials stated they apply the SDLC, as described in DM 3200-001, to their system software development activities. However, we were unable to confirm the extent that RMA had implemented the process, due to the fragmented nature of the formal directive system as it pertained to IT operations and functions. We noted that RMA changed from Application C to Application E for the 2003 reinsurance year without following the required SDLC methodology. These applications generate monthly accounting reports for reinsured companies, and these reports are the basis of exchanges of funds between RMA and the reinsured companies. Although the overall function of the application remained the same, the code used in the application was changed from one computer language to another. The program manager stated that he considered the change in computer code language to be a minor maintenance revision to an existing system rather than, in essence, initiating a new production system for the 2003 reinsurance year. However, we believe that the change in computer language represented a material revision to the application because it involved a reconfiguration of the logic and language used for the entire application rather than just an adjustment of existing code. Also, the program manager was unable to provide adequate documentation to support that the change was made as a part of the maintenance phase of the Departmental SDLC methodology.

Although we did not review RMA's application testing practices for other applications, a contractor procured by RMA for an independent review of its IT operations also cited RMA's inability to apply the SDLC methodology in a report, dated November 15, 2001. The contractor recommended that RMA upgrade the software development processes to provide project management, software quality and

configuration management discipline. RMA indicated they had purchased a configuration management software package to help resolve this issue, but it was left to individual application managers' discretion as to when to use it.

Imbedded Data and File Validation Checks. RMA did not incorporate fundamental data and file validation checks into Application E source code. The responsible manager stated that he believed imbedded validation checks would be redundant and unnecessary because program technicians performed manual validation checks on production data after the application was executed. We believe that manual or visual validation reviews are not as reliable as imbedded validation routines because automated checks are performed automatically before production begins. Manual validations are less reliable since the personnel required to perform them may be distracted by other priorities or absent on the days that the application is executed. As a result, program managers cannot provide reasonable assurance that production data are complete and accurate after production of the monthly financial reports for reinsured companies.

DM 3140-1.3<sup>48</sup> instructs agencies to design and write systems and applications to provide comparison of input controls with data. FIPS 73<sup>49</sup> states that data should be validated continuously as new data are generated or used during processing. It further states that maintaining control totals, completeness, consistency of fields in the record, and a valid sequence of transactions can check a group of records or transactions.

RMA officials stated automated data and file validation checks were completed in Application D, one of its three mission-critical applications. RMA manually verifies the monthly totals in the Application E reports to summary data maintained in the database for Application D. RMA also relies on the reinsured companies to notify them of incorrect data in the monthly accounting reports produced with Application E and submitted to them for validation and attestation. RMA officials believe that manual validation reviews are an adequate substitute for automated validation checks imbedded within the application source code. However, we disagree that these compensating controls are sufficient because the data are not validated continuously while being generated and processed.

Application Software Placed in Production Without Due Analysis of Test Results. RMA placed Application E, one of RMA's three

---

<sup>48</sup> DM 3140-1.3, "Management ADP Security Manual" (March 1992), Part 3 of 8, Section 17.a.4.

<sup>49</sup> FIPS 73, "Guidelines for Security of Computer Applications" (June 1980), Section 3.1.2.

mission-critical applications, into production without adequate analyses of system, operational, or acceptance test results. Although the system administrator tested Application E before it was used for processing production data, he did not analyze the test results to assure prompt identification and correction of any errors or control weaknesses disclosed by the tests before it was placed in production. As a result, RMA has reduced assurance that Application E was operating as intended when deployed. However, we noted no evidence of errors at the time of our review.

The President's Council on Integrity and Efficiency's (PCIE) Review of Application Software Maintenance in Federal agencies, which was issued in September 1996, recognized that software testing is a critical component of software maintenance. The PCIE document also noted that insufficient testing and analysis of test results could result in programs that fail when introduced into the production environment. GAO's Federal Information System Controls Audit Manual states that the extent of software testing should generally vary depending on the type of modification. For major changes, testing should progress through a series of stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing). Because testing is an iterative process that is generally performed at separate levels, it is important that RMA adhere to a formal set of procedures or standards that include requirements for developing a detailed test plan for each change that defines the level of types of tests to be performed along with the responsibilities for the personnel.

In addition to ensuring that application changes are properly authorized and tested, it is also important to obtain final acceptance by user management and other appropriate officials after testing is successfully completed and reviewed. Obtaining such approval helps to ensure that the program changes, along with required database, security, and operational changes are ready for implementation and meet user requirements.

DM 3140-1.3, section 17a (7) states: *“Before any application is placed in production, test the new system, including file maintenance and run recovery, and run in parallel with the old system. Do not discontinue the old system until results are completely acceptable.”*

RMA maintained 2001 production data to execute parallel tests on the 2003 version of Application E. However, the system administrator began using the 2003 version of Application E in October 2002 before technicians fully analyzed the test results. The technicians continued to



analyze test results in March 2003, 5 months after the application was placed in production. Testing also becomes more important with an absence of effective separation of duties, as discussed in Finding No. 1c, which describes that one employee created all source code for Application E, tested and moved the application into production without oversight or quality assurance review, conducted subsequent maintenance on the source code, and was the owner of the directory where the production source code was maintained.

The application manager concurred that Application E was placed in production prior to full analysis of application test results. He also acknowledged that the results were still being analyzed at the time of our review.

### **Recommendation No. 29**

Prescribe and implement in RMA's formal directive system an SDLC methodology in accordance with Departmental regulations and provide senior management oversight to ensure that application managers properly implement the prescribed SDLC methodology and management controls. At a minimum, the controls should include periodic monitoring procedures verifying the implementation of all phases of the Department's SDLC methodology, individual certifications by responsible managers that the methodology was used for each application development project, and a system of quality assurance reviews to ensure that the methodology is applied in accordance with DM 3140-1.3.

#### **RMA Response.**

"RMA concurs. RMA is currently drafting SDLC policies and procedures. Implementation will follow approval."

#### **OIG Position.**

RMA's written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specifics of the SDLC policies and procedures and the estimated timeframes for completion of the planned corrective actions.

---

**Finding 10****Agencywide System and Application Change Controls are Needed**

RMA redeveloped and made other significant changes to in-house application software without applying required controls to ensure that the changes were authorized, appropriate, effective, and efficient. We found the application change activities conducted for one critical application did not include sequentially numbered versions of the application, an appropriate test environment for systems tests, test plans for revisions to application software, sufficiently controlled emergency change requests, or an automated log to document, track, and manage application changes. These conditions occurred because responsible program managers did not adhere to Departmental requirements or develop senior management approved policies and procedures for conducting and controlling changes to RMA applications. As a result, the applications are vulnerable to errors, delays, and interruption of production operations and services.

The Department's SDLC methodology, DM 3200-002,<sup>50</sup> states agencies must use a change control process for all major application systems, properly document the process, and the changes made by it.

We judgmentally selected one of three applications listed by RMA as critical to its mission and two major IT systems for review. We selected Application E because it is used as the basis for exchanging funds between RMA and the reinsured companies. The program manager responsible for this application stated that although his staff did not implement all phases of the SDLC, they applied the maintenance phase. He believed the revisions to the application software were not sufficiently significant to require adherence to the Department's requirements. In a subsequent discussion, a more senior manager agreed with our conclusion that the Department's control requirements were applicable and should have been applied. During the discussion, officials also stated that RMA installed new configuration management software to correct change control weaknesses.

RMA uses an automated project management system to control software changes. However, each business unit is responsible for creating their own procedures. RMA did not have an overall set of formal procedures to ensure there is uniformity between the business units and to ensure all software change requests were properly controlled and executed. For example, the Branch Chief to the Fiscal

---

<sup>50</sup> DM 3200-002, "Management, A Project Manager's Guide to Application Systems Life Cycle Management" (March 3, 1988), Section 1.3B(7).

Systems and Procedures Section provided by e-mail actions and responsibilities for the different parties involved when a software change needed to be completed for Application E. These procedures were not formalized and approved for use by RMA senior management. A subsequent e-mail stated that production emergencies would be reported directly to the computer specialist assigned to the system and action to resolve the production emergency is expected to be taken immediately with the project management-tracking document created after the fact. We did not reconcile the propriety of requests in the project management tracking system other than for Application E.

Version Control. The specialist responsible for maintaining and changing Application E did not sequentially number the various versions of the application as it was revised. This occurred because the application staff relied on backup tapes generated by a mainframe operating system to maintain previous versions of the application. In the event of an emergency or disaster, RMA would not be able to determine if all program specialists used the most current approved version of the application after backup tapes restored the application to generate monthly financial reports.

DM 3200-002<sup>51</sup> states that agencies should maintain a clear, verifiable audit trail of all production library changes. It also states that if there are many changes, group logically, analyze, and make the changes into a change library. Change version numbers should be assigned to logically grouped changes.

The application specialist indicated that a previous version of the application was maintained in the programmer's directory. The names of obsolete application files were not numbered sequentially. Instead, the file names for obsolete versions included an extension of “\_old.” None of the titles or file names for earlier versions of the application included a sequential number to indicate the sequence of application development.

System Tests. RMA maintained a test environment within a production environment to execute application tests while developing a revision to Application E, one of RMA's critical systems. RMA maintained only one system library for application developmental testing, integration testing, and acceptance testing. RMA also did not develop written policy and procedures requiring that separate libraries be maintained for testing and production purposes. The responsible program manager stated that RMA purchased a single license for a commercial software package to operate the application. This precluded RMA from

---

<sup>51</sup> DM 3200-002, “Application Systems Life Cycle Management” (March 1988), Section 1.3.B.7.d and e.

establishing a separate library for testing and production. Thus, the specialist was required to execute application tests within a production environment. The absence of a separate test environment could potentially result in errors, delays, and interruptions to monthly financial reports.

DM 3140-1.3<sup>52</sup> states: *“Before any application is placed in production, test the new system, including file maintenance and run recovery, and run in parallel with the old system. Do not discontinue the old system until results are completely acceptable.”*

We noted that an independent contractor also reported this weakness to RMA in a November 15, 2001, report. The report did not make any specific recommendations to conduct testing within a production environment and did not acknowledge any corrective actions by RMA on this issue. Also, we found no evidence during the audit of corrective actions taken by RMA.

Test Plans. RMA did not prepare test plans or obtain formal user acceptance when developing and implementing Application E to replace Application C. This occurred, in part, because RMA had not fully established appropriate change control policies and procedures requiring that system test plans be developed. As a result, this financial reporting system was more vulnerable to errors, delays, and interruption of production operations and services. The responsible manager stated that employees performing the tests were knowledgeable of the application; therefore, formal test plans and approvals were not necessary.

DM 3200-002<sup>53</sup> provides that the required elements for a test plan include such elements as a functional summary, a schedule of tests and key participants, the resources, methodologies, materials, and procedures to be used. User acceptance testing is a critical phase of any systems project and requires significant participation by the end users. To be of real use, an acceptance test plan should be developed in order to plan precisely, and in detail, the means by which acceptance will be achieved. According to DM 3200-002, the user acceptance stage is a part of the SDLC. During this stage, a written signoff should be obtained from the user acceptor. This signoff shows that the functions and data provided by the systems meet the users requirements. Establishing a user acceptor is an organizational strategy for obtaining user participation. This is an individual appointed at the beginning of system development. This individual is to monitor and

---

<sup>52</sup> DM 3140-1.3 (1984), Part 3, Section 17, Paragraph a.7.

<sup>53</sup> DM 3200-002 (March 1988), Subsection 3.2C(1).

coordinate, from the user prospective, those systems development projects in a user area.

Emergency Changes. We reviewed Application E emergency application change control documentation and found that the only documentation was an informal e-mail from the Branch Chief that authorized change requests, but did not define emergency changes or prescribe timeframes for accomplishing changes. RMA personnel said that the agency had not established formal agencywide policies and procedures for controlling application software change requests and that application managers tailored change controls to the needs of their various RMA applications. As a result, the staff may not respond consistently or timely to a legitimate emergency change request, potentially resulting in delayed or inaccurate production runs.

DM 3200-002<sup>54</sup> also includes general guidance for application change controls. The manual notes that, although the cost of changes must be within the resources budgeted for the operation and maintenance of the system, all major application systems must use a change control process. The process should be properly documented and changes should be made in accordance with the documentation.

System Audit Logs. We found System A did not generate an audit log to track and manage system activities, such as file and application changes, routine maintenance, program executions, and user actions. The responsible manager stated that the audit log was turned off because it slowed the system during production runs. We also found that another mission-critical system did not record changes made to files. Thus, RMA is dependent upon employees and contractors to recall and/or reconstruct changes made to the application software, rather than use system-generated evidence of actual changes. A properly established and maintained audit log would routinely generate a record showing the actions taken, the name and access rights of the persons responsible for the changes, the date and time of each change, and the name of the program changed; however, the log did not define the nature of changes made.

DM 3140-1.3<sup>55</sup> instructs agencies to: *“Provide controls which maintain accounting and access logs sufficient to permit reconstruction of events in case of unauthorized data or program access or use, illegal use of privileged instructions or functions, unexplained program aborts, or questionable processing results.”*

---

<sup>54</sup> DM 3200-002 (Mach 1988).

<sup>55</sup> DM 3140-1.3 (1984), Part 3, Section 16.

In addition, a contractor, procured by RMA for an independent review of its operations, also cited weaknesses in RMA's software development process and systems in a report, dated November 15, 2001. The contractor reviewed a different mission-critical application. However, the contractor's report states "*If RMA were to launch into any major system's redesign or consolidation effort, its designated IT organization would face a high risk of failing to do two critical things in its current state:*

- *create systems that meet the needs and*
- *deliver projects according to schedules and budgets.*"

The contractor's report did not make recommendations relating to the specific Departmental requirements. RMA generally agreed that their systems did not generally use logging tools to manage critical systems activities.

### **Recommendation No. 30**

Consult with the OCIO for guidance and assistance and implement and document RMA system development, maintenance, and change activities in accordance with Departmental change control guidance and direction and ensure the requirements are properly applied on an agencywide basis.

#### **RMA Response.**

"RMA concurs. The Agency is already working with the OCIO on a number of investments and projects that contain the activities discussed in this recommendation."

#### **OIG Position.**

RMA's written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specifics of the actions planned and the estimated timeframes for completion of the planned corrective actions.

### **Recommendation No. 31**

Establish procedures requiring effective senior management oversight to periodically monitor and provide assurance and documentation showing that system logs are properly maintained, operating continuously, and effectively monitored to track and manage system activities.

### **RMA Response.**

“RMA concurs. Oversight responsibilities and processes are being identified as part of the Administrator's Audit Remediation Plan.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specifics of the actions planned regarding senior management oversight and the estimated timeframes for completion of the planned corrective actions.

## **Recommendation No. 32**

Establish procedures requiring effective management supervisory controls and oversight to provide assurance and documentation that the various versions of applications are sequentially numbered and logically grouped and that test plans are prepared and approved for each development stage prior to implementation of the application. Also, conduct periodic reviews to ensure that procedures are followed.

### **RMA Response.**

“RMA concurs. The implementation of both Synergy and Magic for change/configuration management will assure that application software versions are retained and can be recovered. Testing policies and procedures including the level of documentation required and retention of test plans will be outlined. Review processes for all IT procedures are being developed by the CIO's office as part of Agency oversight activities.”

### **OIG Position.**

RMA's written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specifics of the actions planned and the estimated timeframes for completion of the planned corrective actions.

## **Recommendation No. 33**

Purchase and maintain sufficient copies and licenses for commercial software packages to properly maintain, operate, and monitor RMA applications and systems they support in both a testing and production environment.

**RMA Response.**

“RMA concurs. The Agency is implementing an integrated automated budget/procurement/inventory system that will support full lifecycle management of all Agency assets. This will associate software with the owner/user and allow System Administrators to more accurately track copies needed and copies in use.”

**OIG Position.**

RMA’s written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the estimated timeframes for completion of the implementation of the integrated automated budget/procurement/inventory system that will support full lifecycle management of all Agency assets.

**Recommendation No. 34**

Direct the RMA CIO to conduct training for all RMA staff regarding the weaknesses cited herein, and hold senior managers accountable for implementing corrective actions.

**RMA Response.**

“RMA concurs. The Agency will work with the OCIO and OIG to develop a training program for managers, supervisor and staff vested with IT responsibilities.”

**OIG Position.**

RMA’s written comments presented concurrence with the recommendation. To enable us to accept management decision, RMA will need to provide the specifics of the training program and the estimated timeframes for completion of training for managers, supervisor, and staff vested with IT responsibilities.



# ***Scope and Methodology***

---

Our audit was part of a nationwide audit of selected USDA agencies. We tested selected RMA computer networks to identify vulnerabilities that could enable unauthorized users to access sensitive data stored on or transmitted over RMA systems. We conducted our review through interviews, review of RMA procedures and records, and observations. We used commercially available software applications to assist us in our security review of the Kansas City Service Center located in Kansas City, Missouri. RMA and FSA share computer systems in WDC. This software was also used to perform a limited security review of these systems.

We also reviewed controls established on one of three RMA mission-critical IT applications to ensure the integrity of its information security program. To accomplish our audit objectives, we performed the following procedures:

- Gained an understanding of the RMA IT environment;
- Reviewed agency, Departmental, and other federally mandated IT security policies and procedures;
- Interviewed responsible officials for managing RMA's IT systems and mission-critical applications, reviewed RMA records, and made observations;
- Performed detailed testing of RMA's entity-wide security program, logical access controls on two LAN's and one of three mission-critical applications, and software controls by analyzing records and controls established to ensure the security of RMA's computer systems;
- Conducted vulnerability scans on several agency networks using commercially available operating system vulnerability software;
- Conducted a detailed assessment of the security of RMA's network operating systems using commercial software packages to provide comprehensive and flexible reporting capabilities of access control settings, such as user account characteristics and password controls;
- Tested two networks in Kansas City, Missouri. One network included 16 servers, 8 of which were located in Kansas City, Missouri, 8 located in various RMA Regional offices,

and 854 user accounts. Tests of the second network included a server and 193 user accounts; and

- Reviewed the RMA network operating system in WDC. The RMA WDC network was part of a larger network that was administered by FSA. We limited our review to four servers (based on observations by FSA employees of the servers' utility for RMA) and 258 accounts. We immediately communicated the results of our review to RMA management to facilitate prompt corrective action.

Audit fieldwork was performed from November 2002 through April 2003. The audit was conducted in accordance with Government Auditing Standards.

# ***Glossary of Terms***

---

<b><u>Accreditation</u></b>	The formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk.
<b><u>Business Continuity and Contingency Plan (BCCP)</u></b>	Provides guidance and direction to all managers and staff within an agency on action to be taken in the event of disruptions to normal business operations.
<b><u>Certification</u></b>	Security reviews or evaluations, formal or informal, that take place prior to and are used to support accreditation.
<b><u>Configuration Management</u></b>	A process of reviewing and controlling the components of an Information Technology System throughout its life to ensure that the components are well defined and cannot be changed without proper justification and full knowledge of the consequences. Configuration management ensures that hardware, software, communications services, and documentation for a system can be accurately determined at any time.
<b><u>“Denial of Service” Attacks</u></b>	Attempts to slow or shut down targeted network systems or services.
<b><u>Generic/Shared Account</u></b>	User accounts that are accessed by more than one person and are not associated with a particular person.
<b><u>Issue-Specific Policy</u></b>	Developed to focus on areas of current relevance and concern (and sometimes controversy) to an organization.
<b><u>Least Privilege</u></b>	Refers to the security objective of granting users only those accesses they need to perform their official duties.
<b><u>Security Plans</u></b>	Documentation that helps ensure that security is considered not only during system design and development, but also throughout the system’s life cycle. Security plans may also be used to ensure that OMB Circular A-130, Appendix III, and other requirements, are properly addressed.
<b><u>Software Development Lifecycle</u></b>	The time span between establishing a need for a system or application and the end of its operational use. The SDLC is divided into discrete, separate points for management control.

**System Administrator**

The most trusted position on a system. A system administrator has complete control of the system and has unrestricted access to any information on that system, including sensitive information.

**Test Plan**

A plan that should describe what is to be tested and the testing methods or tools to be used. A test plan should include tests that identify the system's response to abnormal, unusual, improbable, and illegal circumstances that may exist during both data input and processing.

**Transmission Control  
Protocol/Internet  
Protocol (TCP/IP)**

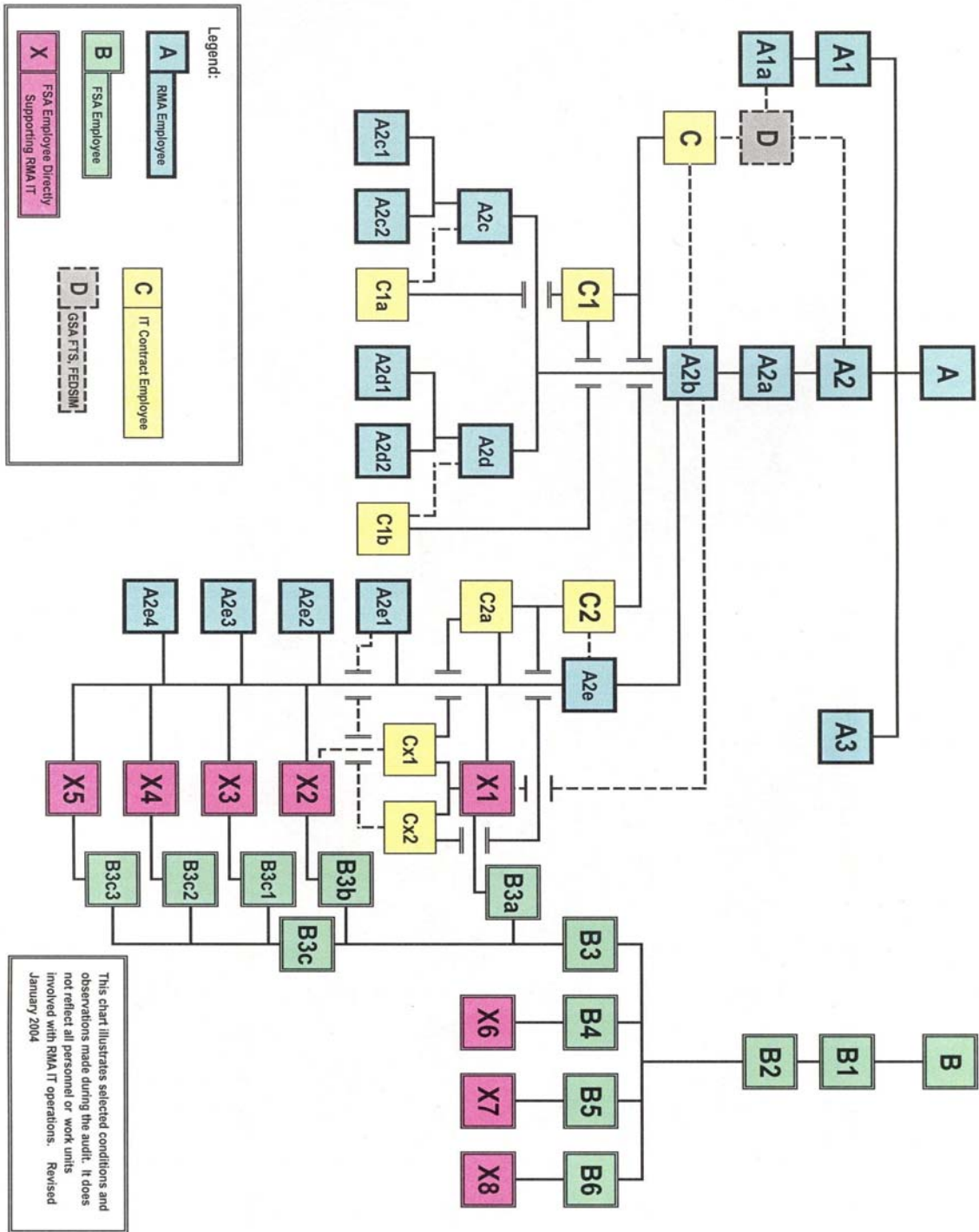
A series of protocols originally developed for use by the U.S. military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms.

**“Unknown User” Account**

A person or entity who obtained a user ID and password without authorization.

# Exhibit A – RMA IT Organizational Chart

As of January 1, 2003



# Exhibit A – Key to RMA IT Organizational Chart

## Risk Management Agency:

**A** Administrator, RMA  
**A1** Chief, Program Support & Acting  
RMA Chief Information Officer  
**A1a** Technology & Special Projects  
Contracting Officer  
**A2** Deputy Administrator, Research  
& Development  
**A2a** Assistant Deputy Administrator,  
Research & Development  
**A2b** Director, Actuarial Division  
**A2c** Chief, Fiscal Systems Branch  
**A2c1** Information Technology Specialist  
**A2c2** System Accountant  
**A2d** Chief, Program Automation Branch  
**A2d1** Information Technology Specialist  
**A2d2** Information Technology Specialist  
**A2e** Chief, System Administration Branch  
**A2e1** Team Leader, Configuration  
Management  
**A2e2** Team Leader, Network Administration  
**A2e3** Team Leader, UNIX Administration  
**A2e4** Team Leader, Database  
Administration  
**A3** Chief, Compliance

## Farm Service Agency:

**B** Administrator, FSA  
**B1** Deputy Administrator, Management  
**B2** FSA Chief Information Officer  
**B3** Information Technology Systems  
Technology Office, Kansas City  
**B3a** Information Systems Security  
Program Manager, Kansas City  
**B3b** Chief, Network Management Branch  
**B3c** Telecommunications Division  
**B3c1** FSA Help Desk, Kansas City  
**B3c2** Chief, Hardware Management Branch  
**B3c3** Chief, Software Management Branch  
**B4** Chief, Policy and Planning Branch  
**B5** Chief, Customer Services &  
Operations Branch  
**B6** Chief, Systems Development Branch

**X1** RMA Information Systems Security  
Program Manager, Kansas City  
**X2** Team Leader, RMA Network  
Administration, Kansas City  
**X3** Information Technology Specialist,  
Kansas City  
**X4** Information Technology Specialist,  
Kansas City  
**X5** Information Technology Specialist,  
Kansas City  
**X6** Information Systems Security  
Program Manager, Washington  
**X7** LAN Management Section,  
Washington  
**X8** Executive Management Systems  
Section, Washington

## Science Applications International Corporation:

**C** Project Manager, RMA Millennium  
Contract  
**C1** Software Integration Manager  
**C1a** Team Leader, Accounting  
Applications  
**C1b** Team Leader, Data Acceptance  
System  
**C2** Systems Integration Manager  
**C2a** Contract Lead, Network  
Administration  
**Cx1** Security Engineer/Network Analyst  
**Cx2** Security Engineer/Contract Lead,  
Configuration Management

## U.S. General Services Agency:

**D** Federal Systems Integration and  
Management Center

# Exhibit B – RMA Response to the Draft Report




United States  
Department of  
Agriculture

Risk  
Management  
Agency

1400 Independence  
Avenue, SW  
Stop 0801  
Washington, DC  
20250-0801

APR 14 2004

TO: Robert W. Young  
Assistant Inspector General for Audit  
Office of Inspector General

FROM: Michael Hand   
Agency Audit Liaison Official

SUBJECT: OIG Audit 05099-18-KC: Risk Management Agency (RMA) and Security  
of Information Technology Resources

Outlined below is RMA's response to the recommendations within the subject audit.

### Recommendation 1:

*Delegate sufficient authorities and provide adequate staff and other resources to the CIO to develop and oversee an effective IT system, organization, and operation, and to properly manage and administer RMA IT security activities.*

### RMA's Response:

RMA conditionally concurs. Senior Management has reviewed current IT authorities and resources. A draft proposal addressing this recommendation is currently under review. OIG and the OCIO will be provided with the document once approved.

### Recommendation 2:

*Reorganize the RMA's IT organization structure to ensure the independence of the CIO and the IT security staff from control and improper influence by production managers.*

### RMA's Response:

RMA conditionally concurs. Senior Management is analyzing the current IT organizational structure, including issues related to the CIO and security staff. A draft proposal will be issued for review in the near future. The document will be distributed to OIG and the OCIO once approved.

### Recommendation 3:

*Renegotiate and revise the reimbursable agreement with FSA to reflect planned changes in RMA's IT organizational structure and internal operations. The agreement should include sufficiently detailed descriptions of the services to be provided so that the IT responsibilities of both agencies are clearly understood by the employees charged with carrying them out, as well as by agency managers, employees, and other parties, as needed.*

**RMA's Response:**

RMA concurs. As discussed during the audit, FSA is currently divesting itself of all interagency support functions as part of the move to the service center (SCITO). RMA is currently negotiating with FSA regarding the return of functions, personnel and budget. RMA has rewritten the Memorandum of Understanding for renegotiation in the event SCITO negotiations are cancelled.

**Recommendation 4:**

*Immediately develop, document and implement appropriate written policies and procedures that have been reviewed and approved by responsible senior management covering all RMA IT security operations, processes, functions, and activities and include these policies in handbooks to be provided and used by all managers, system administrators, security officers, developers, contractors, and IT users. The handbooks should provide RMA IT policies, assign IT responsibilities, and identify the management controls that shall be implemented to protect RMA's IT resources and ensure they are functioning as needed.*

**RMA's Response:**

RMA concurs. However, it should be noted that policies for seven broad IT areas were drafted, distributed and put in place before the audit, however, they did lack the CIO's signature. The policies were approved by two levels of management, put in force and were being monitored to assure adherence. Violations were reported to the ISSPM (Information Systems Security Program Manager or Agency Security Officer) and escalated up the management chain (including to the OCIO Office of Cyber Security when appropriate). All that was lacking was the "official" signature of the Administrator or CIO.

RMA continues to implement new policies and to conduct regular reviews of current policies.

**Recommendation 5:**

*Prescribe and apply a periodic monitoring review process to ensure that approved policies and procedures for RMA IT operations, processes, functions, and activities are properly and consistently applied and continuously enforced agency wide.*

**RMA's Response:**

RMA concurs. RMA's CIO, System Administration Chief and Security Officer and staff are systematically analyzing and documenting enforcement mechanisms (automated and manual) for Agency IT policies and procedures. These will be incorporated into the CIO's IT Internal Control Manual. Processes will include recording and retaining checklists, reports, etc. for auditor review beginning in FY 2005.



**Recommendation 6:**

*Utilize this report to identify and include RMA IT organizational and security weaknesses in RMA's annual FMFIA report and in subsequent FMFIA reports until all material weaknesses have been corrected and IT operations substantially comply with applicable laws and regulations.*

**RMA's Response:**

RMA conditionally concurs. As discussed during the audit, not every weakness identified by OIG directly affects the Agency's financial systems. Weaknesses, recommendations and findings that directly relate to the health of these systems will be reported in the annual FMFIA report.

**Recommendation 7:**

*Develop, document, and implement an action plan with milestone dates for an overall strategy to address the weaknesses not cited in RMA FMFIA reports.*

**RMA's Response:**

RMA concurs. The Administrator, in conjunction with the CIO, has already put into place an Audit Remediation Plan that includes every open item in the recent Security and Financial audits. Additionally, the Fiscal Operations and Systems Division and CIO management team are also incorporating related action items into the 5-Year FMS Plan as well as their own internal FMFIA Remediation Plan.

**Recommendation 8:**

*Prepare and submit quarterly status reports to OCIO until the cited weaknesses in FMFIA reviews and reporting, risk assessments, system certifications, security plans, contingency planning and disaster recovery, background investigations, incident response procedures, security training, performance measures, and unauthorized software are corrected.*

**RMA's Response:**

RMA concurs. RMA will provide the OCIO with quarterly summaries of activities completed and pending under the Audit Remediation Plan.

**Recommendation 9:**

*Strengthen senior management oversight and periodically monitor and document the effectiveness of agency wide policies, procedures, and management controls to ensure that IT services contract provisions conform to all applicable laws and regulations and that contract provisions are enforced.*

**RMA's Response:**

RMA concurs. See Agency response to recommendations 3 and 5.

**Recommendation 10:**

*Require background investigations for all IT contractor employees and associated subcontractor employees, where applicable, and ensure they are satisfactorily completed before access to RMA systems, hardware and facilities are authorized.*

**RMA's Response:**

RMA concurs. The Agency is currently conducting background investigations on the most recent contractor hires. Background clearance for older contractor hires will be completed this FY. Federal employees will be investigated in the coming 24 months as budget allows. Language regarding the ongoing requirement for background checks has been submitted to GSA for incorporation within the Millennium contract.

**Recommendation 11:**

*Improve and document senior management oversight to ensure that Federal employees do not supervise the day-to-day activities of contracted security specialists and other IT contractor employees and to ensure adequate separation of duties and responsibilities assigned to individual contractor employees.*

**RMA's Response:**

RMA conditionally concurs. RMA disagrees with some statements regarding direct supervision of contractors. Federal employees serve as leads, escalation points and technical representatives at some junctures in the contracting process. Typically, contractors have standing duties assigned to them by the contract company, such as ongoing monitoring and maintenance. RMA leads are not assigning work, however they provide the Agency's approval for work efforts to take place in effect authorizing work for billing.

RMA will issue a document and training materials reminding employees of applicable regulations and proper conduct in relation to contracting. RMA will further document and regulate interaction between Agency officials and contracting staff and/or management to remove the perception of direct supervision of contractors.

**Recommendation 12:**

*Prepare individual task orders and other supporting documentation, as needed, to describe the specific security services expected from contractor employees and to record the details of the services or deliverables to be provided by them.*

**RMA's Response:**

RMA concurs. RMA has already supplied the contracting firm and GSA with security tasking requirements in writing. These will be incorporated into the Millennium contract and have already been utilized to fill the current positions.

**Recommendation 13:**

*Take immediate action to correct all high and medium-risk vulnerabilities identified by our vulnerability scans and conduct rescans to ensure that the vulnerabilities identified by us have actually been corrected. Require IT officials to track each vulnerability and certify that actions have been taken to remedy the problem for all vulnerabilities identified by our scans.*

**RMA's Response:**

RMA conditionally concurs. Undisputed vulnerabilities will be corrected. Though the audit document indicates 306 medium and high-risk vulnerabilities, some vulnerabilities are disputed. For example, Novell users are not flagged as active when they dial-in. For a number of remote users, they will only be dial-in customers. These were picked up as "inactive accounts" by the scans. Novell cannot be reconfigured; it is a nuance of the environment.

**Recommendation 14:**

*Require IT officials to run vulnerability scans of the RMA's entire network on a monthly basis to detect, track, and correct noted vulnerabilities. Establish a comprehensive plan that will assure effective testing of RMA's network so that data is safeguarded and assess low-risk vulnerabilities to identify trends and initiate actions on those areas in the aggregate that could lead to more serious vulnerabilities.*

**RMA's Response:**

RMA concurs. Scans were run, however insufficient man-hours were available to review results and document findings. While some reviews were conducted, they were not performed at regularly scheduled intervals and historical logs and findings were not retained for audit team review. As part of the Administrator's Audit Remediation Plan, the Agency is reviewing automated tools to support this process. Though automated tools will help facilitate this function, funding of additional manpower in FTE or contractors will be required.

**Recommendation 15:**

*Require IT officials to develop and follow a configuration management program for RMA's systems. Assure periodic tests are performed and tracks and correct items identified and ensure that the plan is in place and operating effectively. Codify descriptive management policies and procedures for these operations in RMA's directive systems.*

**RMA's Response:**

RMA concurs. RMA has purchased and is implementing change/configuration management tools within both the business systems (Synergy) and the infrastructure (Magic Solutions) environment. RMA is also instituting uniform policies and procedures across the business systems and infrastructure for change/configuration that will include a Change Control Board as well as a fulltime Change/Configuration Management Officer.

**Recommendation 16:**

*Develop and apply a policy to conduct a routine and timely review of RMA's firewall configuration and periodically verify the effectiveness of FSA firewall protection that RMA must rely upon.*

**RMA's Response:**

RMA concurs. The System Administration Chief and Security Team are currently implementing processes that include periodic reviews supplemented by software that performs ongoing automated monitoring of firewall effectiveness.

**Recommendation 17:**

*Review the Washington, D.C., firewall configuration and placement to ensure the FSA firewall adequately protects the RMA network from intruders periodically re-verify that the RMA network is adequately protected in the future.*

**RMA's Response:**

RMA concurs. RMA is currently implementing the Cable Plant Project, which reconfigures RMA's access into and out of the USDA backbone within the DC office. It will allow the RMA to more strictly control access instead of deferring to Farm Service Agency access controls. Until such time as the WDC Migration is completed, the RMA will request that FSA Pacific and PTX firewalls be periodically tested for penetration vulnerabilities.

**Recommendation 18:**

*Correct the cited network vulnerabilities disclosed in this finding. Also, develop and implement formal written policies establishing minimum security setting and user configuration guidelines for RMA networks, periodically reassessing those settings and user configurations, and establishing a process to ensure the correction of those settings and configurations found to be misapplied.*

**RMA's Response:**

RMA conditionally concurs. Vulnerabilities not identified and disputed in this document

will be corrected. RMA disputes the SNMP vulnerabilities cited. RMA regularly uses this protocol for Internal Network Management to manage internal switches, routers, and other network devices. We block all other access into our network (With the exception of OCIO Read Only permissions) for SNMP. Written policies and procedures to address the deficiencies are currently being drafted. Ongoing monitoring processes will be instituted upon approval of the policy.

**Recommendation 19:**

*Identify the user for the "Unknown User" account with unrestricted access to RMA's servers. Depending on the identification of the user, either configure the system to maintain the identity for that user internally, or file an incident report with OCIO regarding security weaknesses of the systems that allowed the condition to exist.*

**RMA's Response:**

RMA does not concur. Auditors were briefed on the fact that the "unknown account" in the Windows 2000 domain (OP) was the enterprise administrator account in the "placeholder" (RM) domain. The OP domain could not resolve the account because it does not exist in the OP domain. The account has full privileges in the OP domain because of the nature of Windows 2000 Active Directory.

**Recommendation 20:**

*Develop internal written policies and procedures that establish effective access controls for RMA-controlled users to follow in using RMA, NITC, and NFC systems in accordance with applicable Federal guidance and DR requirements. Conduct periodic reviews to ensure RMA user compliance with the policies and procedures implemented.*

**RMA's Response:**

RMA conditionally concurs. RMA will develop the policies and procedures discussed in recommendation 20, however, RMA still disputes findings related to NFC as their systems are outside RMA control.

**Recommendation 21:**

*Evaluate the user accounts cited as dormant, lapsed, or unnecessary and deactivate those without confirmed justification for the remaining active accounts. Also, develop and implement a workable methodology to periodically review the activity of all user accounts to promptly identify and remove unnecessary accounts.*

**RMA's Response:**

RMA concurs. Problem accounts identified in the course of the audit have already been

researched and removed as appropriate. The Security Team is implementing an automated process combining several tools such as Magic and Tripwire to further improve tracking and removal of inactive accounts.

**Recommendation 22:**

*Develop and implement an effective process to promptly identify and terminate user accounts and system access to all RMA systems when employees and contractors are separated from RMA employment and/or service, as applicable. This process should entail RMA management and/or supervisors being accountable for notifying the security office of employees or contractors being separated.*

**RMA's Response:**

RMA concurs. The agency is taking measures to improve tracking of inactive accounts and reporting of transfers, terminations and other events that trigger a change in security status for employees and/or contractors.

**Recommendation 23:**

*Terminate all generic and shared accounts and establish a policy to prohibit their use in the future. Implement a process to periodically review accounts to verify that only one person is accountable for all access and activities performed with or through each user account.*

**RMA's Response:**

RMA does not concur. Auditor analysis regarding "Generic or Shared Accounts" is incorrect. RMA technicians explained the difference between a generic account, a shared account, and a service account, as defined by RMA, Microsoft, Sun, and other IT companies. A service account is used by the system to run applications such as email or databases. By nature, these accounts will have passwords that do not expire because the account is not "owned" by any individual. No "person" knows or holds the password; therefore, an administrator has to change the password. When new passwords are needed, they are generated by the system, making them superior to passwords created by a human. It is RMA policy to obscure the names of these accounts by naming them something other than system specific or service specific names (e.g., administrator or SQLAdmin).

**Recommendation 24:**

*Immediately remove dial-in access for generic accounts and unknown or unidentified users. Also, establish effective controls, such as periodic reviews, to ensure dial-in access is needed, secured, approved, maintained, and periodically monitored to ensure only one user per account. Terminate authorization for dial-in access promptly after the need for access has ended.*

**RMA's Response:**

RMA conditionally concurs. Periodic reviews of all accounts and their access level will be instituted as will a more reliable account termination processes. There is dispute regarding generic accounts and unknown and unidentified users. Auditors were briefed on the fact that the "unknown account" in the Windows 2000 domain (OP) was the enterprise administrator account in the "placcholder" (RM) domain. The OP domain could not resolve the account because it does not exist in the OP domain. The account has full privileges in the OP domain because of the nature of Windows 2000 Active Directory. The document overstates the kind and number of weaknesses related to password and ID administration. This is due, in part, to a difference in interpretation between RMA and OIG technicians including a dismissal of the nuances between operating systems. For example, OIG determined excessive unused accounts. Even after discussion about the nuances of Novell, and the fact that Novell does not log remote users as active nor can you make Novell log remote users as active this was still reported as a problem condition.

**Recommendation 25:**

*Establish controls to ensure that user rights and privileges are limited to those necessary for each user to fulfill his/her duties and responsibilities. These controls should include a central inventory file showing the rights and privileges authorized for each user on each system that is maintained and requirements that the file be periodically previewed by RMA managers, supervisors, and the Security Officer, to ensure rights and privileges are current.*

**RMA's Response:**

RMA concurs. To remedy this problem, RMA will be utilizing a segregated security database within the Magic tool. Security levels will be tracked and matched against system components. Unauthorized changes will be identified via Tripwire and reported to the appropriate security and system administration personnel. The Administrator has approved a full-blown reassessment of access for every employee and contractor. This process will establish and record the new baseline in the automated system.

**Recommendation 26:**

*Restrict physical access to RMA IT system hardware to only RMA employees and contractors with an ongoing recurring business need for unescorted access to restricted IT spaces. Conduct periodic monitoring of personnel granted access to the cited computer room and ensure only authorized personnel fare granted access.*

**RMA's Response:**

RMA concurs. RMA is working with FSA ASD to remedy this deficiency. Separation of the RMA/FSA facilities is contingent on cost analysis by FSA ASD to expand computer room space and RMA's ability to fund its share of the expansion.

**Recommendation 27:**

*Establish a procedure requiring authorized database personnel to log the removal and return of system tapes to and from system libraries. Also, require periodic reviews to ensure the procedure is implemented and logs are properly maintained.*

**RMA's Response:**

RMA conditionally concurs. RMA has taken steps to improve backup and recovery processes including the check-in, check-out, logging and storage of tapes and other media. These functions are outlined in SAB operating procedures and have been vested in SAB Operators, however these individuals are not "database personnel" per se.

**Recommendation 28:**

*Establish a formal policy and conduct periodic reviews to ensure that equipment security cages are locked when authorized personnel do not require immediate access and keys are controlled to ensure they are always recovered before personnel are separated from employment or from needing access.*

**RMA's Response:**

RMA concurs. RMA will institute a spot-check procedure to monitor that security cages are properly locked and that keys are secured and only accessible to authorized personnel. This work has begun, and is ongoing. In February of 2004, the Network Group locked all Server racks, and stowed keys in safe locations. During the March Maintenance Weekend, the primary RMA Router Rack was upgraded to a front/back locking rack with keys stowed in safe and secure locations. The remaining racks will be converted on an ongoing basis in the coming months. In an effort to more strictly control access a key box is being procured; security staff will log in and check out keys to administrators.

**Recommendation 29:**

*Prescribe and implement in RMA's formal directive system an SDLC methodology in accordance with Departmental regulations and provide senior management oversight to ensure that application managers properly implement the prescribed SDLC methodology and management controls. At a minimum, the controls should include periodic monitoring procedures verifying the implementation of all phases of the Department's SDLC methodology, individual certifications by responsible managers that the methodology was used for each application development project, and a system of quality assurance reviews to ensure that the methodology is applied in accordance with DM-3140-1.3.*

**RMA's Response:**

RMA concurs. RMA is currently drafting SDLC policies and procedures. Implementation will follow approval.



**Recommendation 30:**

*Consult with the OCIO for guidance and assistance and implement and document RMA system development, maintenance, and change activities in accordance with Departmental change control guidance and direction and ensure the requirements are properly applied on an agency wide basis.*

**RMA's Response:**

RMA concurs. The Agency is already working with the OCIO on a number of investments and projects that contain the activities discussed in this recommendation.

**Recommendation 31:**

*Establish procedures requiring effective senior management oversight to periodically monitor and provide assurance and documentation showing that system logs are properly maintained, operating continuously, and effectively monitored to track and manage system activities.*

**RMA's Response to Recommendation 31:**

RMA concurs. Oversight responsibilities and processes are being identified as part of the Administrator's Audit Remediation Plan.

**Recommendation 32:**

*Establish procedure requiring effective management supervisory controls and oversight to provide assurance and documentation that the various versions of applications are sequentially numbered and logically grouped and that test plans are prepared and approved for each development stage prior to implementation of the application. Also, conduct periodic reviews to ensure that procedures are followed.*

**RMA's Response:**

RMA concurs. The implementation of both Synergy and Magic for change/configuration management will assure that application software versions are retained and can be recovered. Testing policies and procedures including the level of documentation required and retention of test plans will be outlined. Review processes for all IT procedures are being developed by the CIO's office as part of Agency oversight activities.

**Recommendation 33:**

*Purchase and maintain sufficient copies and licenses for commercial software packages to properly maintain, operate, and monitor RMA applications and systems they support in both a testing and production environment.*

**RMA's Response:**

RMA concurs. The Agency is implementing an integrated automated budget/procurement/inventory system that will support full lifecycle management of all Agency assets. This will associate software with the owner/user and allow System Administrators to more accurately track copies needed and copies in use.

**Recommendation 34:**

*Direct the RMA CIO to conduct training for all RMA staff regarding the weaknesses cited herein and hold senior managers accountable for implementing corrective actions.*

**RMA's Response:**

RMA concurs. The Agency will work with the OCIO and OIG to develop a training program for managers, supervisor and staff vested with IT responsibilities.

If there are any questions regarding RMA's response to the subject audit, please contact Heather Escobar at (202) 690-5886.

