



U.S. Department of Agriculture



Office of Inspector General
Southwest Region

Audit Report

Agricultural Marketing Service Livestock Mandatory Price Reporting System - Application Controls

Report No. 01099-4-Te
December 2004



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



DATE: December 22, 2004

REPLY TO

ATTN OF: 01099-4-Te

SUBJECT: Livestock Mandatory Price Reporting System - Application Controls

TO: A. J. Yates
Chief
Agricultural Marketing Service

ATTN: David Lewis
Director, Compliance Staff
Agricultural Marketing Service

This report presents the results of the subject audit. Your response to the official draft report, dated December 1, 2004, is included in its entirety as exhibit A with excerpts and the Office of Inspector General's position incorporated into the Findings and Recommendations section of the report. Your response contained sufficient justification to reach management decisions on all recommendations contained in the report.

Please follow Departmental and your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer, Director, Planning and Accountability Division. Final action on the management decisions should be completed within 1 year of the date of the management decisions to preclude being listed in the Department's annual Performance and Accountability Report.

We appreciate the courtesies and cooperation extended to us by members of your staff during the audit. If you have any questions, please contact me at 720-6945, or have a member of your staff contact Richard J. Davis, Director, Administration and Finance Division, at 720-1918.

/s/ R. W. Young
ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Agricultural Marketing Service

Livestock Mandatory Price Reporting System - Application Controls

(Report No. 01099-4-Te)

Results in Brief

This report presents the results of our application controls audit of the Agricultural Marketing Service's (AMS) Livestock Mandatory Price Reporting System (LMPRS). Our objective was to evaluate whether AMS had adequate controls over the input, processing, and output of LMPRS data. These controls include ensuring the authorization, completeness, and accuracy of the LMPRS data. AMS relies on LMPRS to provide information on pricing, contracting for purchase, and supply and demand conditions for livestock, livestock production, and livestock products, that can be readily understood by producers, packers, and other market participants. Overall, we found that AMS had authorization, completeness, and accuracy controls for LMPRS data; however, the controls need to be improved.

The LMPRS application owner is the Livestock and Grain Market News Branch (MNB) of AMS. We found that MNB did not have adequate LMPRS application controls including access controls, technical documentation for the application, mandatory report modification process, supervisory reviews, and application monitoring. LMPRS access controls were not limited to the least privilege concept, defined as granting only the access required for a user's job responsibilities. While the technical system documentation for LMPRS is extensive, it did not provide a complete view of all files and database tables used within each module of the application. LMPRS reports were modified by MNB reporters, and there was no second-party review before the reports were posted on the AMS website. There were no routine supervisory reviews of MNB reporters' work and no documentation of reviews that were performed. Reviews of the daily LMPRS operation needed to be improved including monitoring logs and authorized user tables. Therefore, LMPRS application had an increased vulnerability in several areas that could result in unauthorized access and errors in mandatory reports that were posted on the AMS website for the public's use. However, there was no evidence that any instances of unauthorized access have occurred. During our fieldwork, MNB initiated action to ensure LMPRS user access was based on least privilege.

We also found that MNB did not have adequate management controls to ensure that Federal and Departmental guidance on information technology issues was implemented. The LMPRS security plan did not meet Federal and Departmental requirements, including warning banner displays, password expiration, and the locking out of administrator accounts. In addition,

MNB had not submitted any of the required data to address identified weaknesses for the agency Plan of Action and Milestones. MNB also was not performing scans of the LMPRS network. MNB was not aware of these requirements, and the AMS Chief Information Officer had not made it a practice to provide information on these items unless a request was received due to the workload and loss of staff. We also found that the LMPRS application had not been certified before it went into production in April 2001. Officials did not adhere to Departmental guidance and stated that application certifications were not a priority throughout the Government at that time. The absence of a system certification increases the risk that the LMPRS application could be vulnerable to security breaches and cyber-related attacks. During our fieldwork, MNB corrected one security plan deficiency (banner display). They also instituted scans for LMPRS application servers.

Recommendations In Brief

We recommend that AMS:

- Establish and implement application controls to strengthen access privileges, report modifications, supervisory reviews, technical documentation, and application monitoring.
- Establish and implement management controls to ensure that Federal and Departmental guidance is followed regarding the security plan, Plan of Action and Milestones, application certification, and scans.

Agency Response

In a letter dated December 1, 2004, and subsequent correspondence, AMS concurred with all of the findings and recommendations and provided proposed actions and completion dates for each recommendation. (See exhibit A.)

OIG Position

We accept the management decisions for all of the recommendations contained in the report. For final action, AMS needs to provide the Office of the Chief Financial Officer, Director, Planning and Accountability Division (OCFO/PAD), documentation as outlined in the Office of Inspector General's (OIG) Position sections of the report.

Abbreviations Used in This Report

ADP	Automated Data Processing
AMS	Agricultural Marketing Service
CIO	Chief Information Officer
DM	Departmental Manual
GAO	Government Accountability Office
IT	Information Technology
LMPRS	Livestock Mandatory Price Reporting System
MNB	Livestock and Grain Market News Branch of AMS
NIST	National Institute of Standards and Technology
OCFO/PAD	Office of the Chief Financial Officer, Director, Planning and Accountability Division
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
USDA	U. S. Department of Agriculture

Table of Contents

Executive Summary	i
Abbreviations Used in This Report.....	iii
Background and Objectives.....	1
Findings and Recommendations.....	3
Section 1 Application Controls Need Improvement	3
Finding 1 LMPRS Application Controls Were Inadequate	3
Recommendation No. 1.....	7
Recommendation No. 2.....	8
Recommendation No. 3.....	8
Recommendation No. 4.....	9
Recommendation No. 5.....	9
Recommendation No. 6.....	10
Section 2 Management Controls Need Improvement.....	11
Finding 2 Information System Documentation and Policies Need Improvement.....	11
Recommendation No. 7.....	15
Recommendation No. 8.....	15
Recommendation No. 9.....	16
Recommendation No. 10.....	16
Recommendation No. 11.....	16
Recommendation No. 12.....	17
General Comments	18
Scope and Methodology.....	19
Exhibit A – Agency Response	21

Background and Objectives

Background

Application controls are the structure, policies, and procedures that apply to separate, individual application systems. An application system is typically a collection or group of individual computer programs that relate to a common function. In the Federal Government, some applications may be complex, comprehensive systems involving numerous computer programs and organizational units, such as those associated with benefit payment systems. Application controls can encompass both the routines contained within the computer program code and the policies and procedures associated with user activities, such as manual measures performed by the user to determine that data was processed accurately.

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

- Input—data are authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner.
- Processing—data are properly processed by the computer and files are updated correctly.
- Output—files and reports generated by the application actually occur and accurately reflect the results of processing and reports are controlled and distributed to the authorized users.

AMS' LMPRS Application

The U.S. Department of Agriculture's (USDA) Agricultural Marketing Service (AMS) administers programs that facilitate the efficient, fair marketing of U.S. agricultural products, including food, fiber, and specialty crops. AMS includes six commodity divisions: Cotton, Dairy, Fruit and Vegetable, Livestock and Feed, Poultry, and Tobacco.

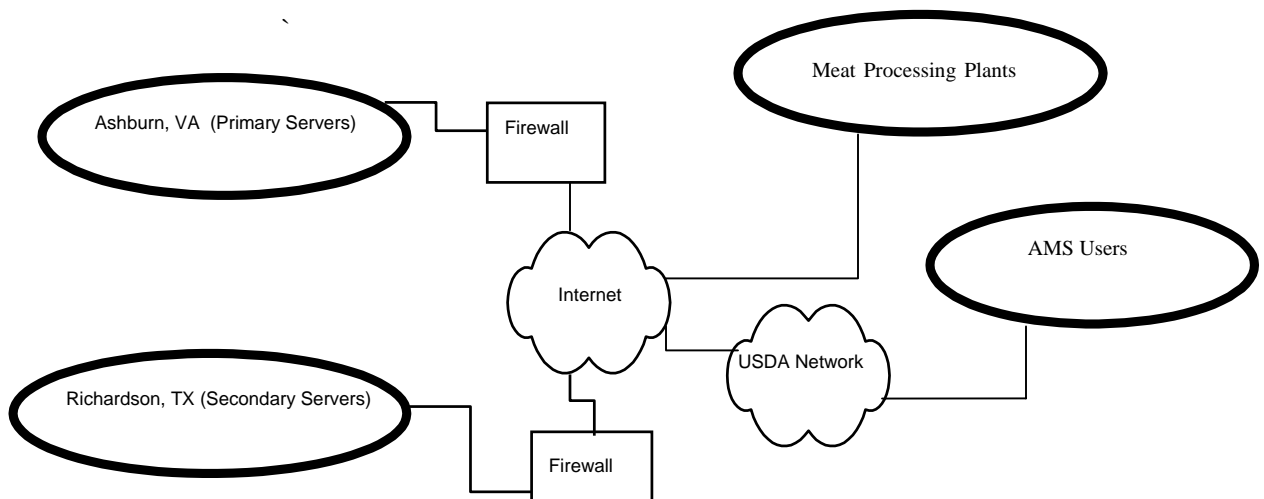
AMS' Livestock Mandatory Price Reporting System (LMPRS) contains information about livestock pricing, contracting arrangements, and supply and demand conditions. The Livestock and Grain Market News Branch (MNB) of AMS implemented the LMPRS in April 2001 in response to the Livestock Mandatory Reporting Act of 1999 (Act), part of the Fiscal Year 2000 Agricultural Appropriation Bill. Under the Act, larger livestock packers, processors, and importers electronically report certain market information regarding transactions of cattle, swine, lamb, and livestock products to USDA. LMPRS is designed to collect the information and summarize it in the form of national reports, which are available to the public on the AMS website.

Approximately 134 meat processing plants submit mandatory data to the LMPRS application on a daily and weekly basis. At least two times each day, reporters in the MNB field offices in Des Moines, Iowa, and St. Joseph, Missouri, manually import the market information received from the plants into the LMPRS production database. The reporters have approximately 1 hour from importing the data to create reports and post them to the AMS website.

The LMPRS application servers are located at two sites - Ashburn, Virginia (primary servers), and Richardson, Texas (secondary servers). The LMPRS network is external to the Department's network, which was unable to accommodate LMPRS activity.

Three contractors and one subcontractor support the LMPRS application. The application contractor developed and maintains the application and is also the system administrator for the LMPRS application. The facility contractor stores AMS-owned servers and other hardware on its property in a secure and protected room. The hardware maintenance contractor provides maintenance functions for hardware switch configuration and supports the firewalls used to protect the LMPRS application. The firewall subcontractor manages the LMPRS firewall and intrusion detection systems.

The following diagram illustrates the data flow of the LMPRS application:



Objective

The objective of this audit was to determine whether AMS had established adequate controls to ensure that data entered into LMPRS are properly authorized, completely processed, and accurately processed.

Findings and Recommendations

Section 1 Application Controls Need Improvement

Finding 1

LMPRS Application Controls Were Inadequate

Our review of LMPRS application controls disclosed several weaknesses involving the assignment of access privileges, reviews by supervisors of modified reports, technical documentation, reviews and documentation of reporter's daily activities, and reviews of the daily operations of the LMPRS application. The causes of the weaknesses in each of the five areas are outlined in the sections below. As a result, the LMPRS application has an increased vulnerability in several areas that could result in unauthorized access and errors in mandatory reports that are posted on the AMS website. (Although, we did not identify any instances of unauthorized access.)

Access Controls

An excessive number of LMPRS users had access privileges that exceeded the needs of their job responsibilities. Inadequate internal controls allowed MNB staff to routinely assign the same access privilege to internal users without considering the users' job responsibilities. As a result, the LMPRS application had an increased risk of unauthorized use, such as the creation and deletion of valid/invalid users or unauthorized access to valid LMPRS accounts.

Federal,¹ Departmental,² and National Institute of Standards and Technology (NIST)³ guidance state users should be granted access based on the least privilege concept. Least privilege refers to the security objective of granting users only those accesses they need to perform their official responsibilities.

Access controls over system and application data include both physical and logical controls and should provide reasonable assurance that computer resources (data files, application programs, and computer equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Logical access controls, such as user names, passwords, and access permissions, ensure that only authorized users have access to network resources from their workstations, and that users are granted only the access that is needed to conduct their job responsibilities.

¹ Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources," section A, dated November 28, 2000

² Departmental Manual (DM) 3140-1, Management ADP Security Manual, Appendix D, section 7 - Vulnerability to Unauthorized Disclosure, dated July 19, 1984

³ NIST SP800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 10, section 10.2.1, dated October 1995

There were three groups of users who accessed LMPRS: AMS users⁴ (47 user accounts), meat processing plant users (134 user accounts), and LMPRS system administrators (4 user accounts - all application contractors). AMS and meat processing plant user accounts are created and deleted by MNB information technology (IT) specialists. Meat processing plant users have a “plant” access profile, which allows limited privileges. An AMS user can have a “reporter” access profile, an “administrator” access profile, or a “reporter/administrator” profile. An LMPRS user with the “administrator” access profile is allowed to modify users and passwords for the LMPRS application. The type of profile is chosen when MNB IT specialists create the AMS user account.

MNB staff stated that they routinely gave AMS users both “reporter” and “administrator” access profiles. We found 36 of 47 AMS users had “administrator” access profiles. MNB stated that this had occurred due to the need to allow the reporters access to other data that was needed for their job responsibilities and because the staff routinely gave both profiles to AMS users. In a prior audit report,⁵ OIG found that least privilege was an issue for other AMS applications that were reviewed. During our fieldwork, MNB modified which AMS users were allowed access to the LMPRS application and had the contractor modify the users’ access profiles. After the modifications, there were nine users with the “reporter/administrator” profile (six AMS users and three application contractors) whose job responsibilities required the access profile.

Report Modification

Some LMPRS application reports were routinely modified and posted on the website without further review. MNB did not have adequate internal controls to ensure that modified reports were subject to a second-party review by reporters’ peers before being published on the AMS website. The supervisors considered the reporters experts and did not feel a review was necessary. As a result, there was an increased risk of errors in the mandatory reports posted on the AMS website for public use.

MNB desk procedures require reporters to review the reports they produce before posting on the AMS website. Reporters work in pairs and review portions of each other’s work. However, the desk procedures did not require second-party review of reports before they were posted on the website. Federal guidance⁶ states internal controls should provide reasonable assurance that the objectives of the agency are being achieved, including reliability of reports for internal and external use, and should be designed to assure that ongoing monitoring occurs in the course of normal operations. Internal controls should be performed continually and be ingrained in the

⁴ AMS users consist of AMS Audit Review and Compliance Auditors and MNB users.

⁵ Audit Report No. 01099-1-FM, “Security Over Information Technology Resources at the Agricultural Marketing Service,” dated March 2002

⁶ Government Accountability Office (GAO), Standards for Internal Control in the Federal Government, Introduction and Monitoring Sections, dated November 1999

agency's operations, including regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

During our fieldwork, we observed the modification of two daily mandatory reports before they were posted on the AMS website. A trend number for a swine report was manually calculated and then changed, and data for a boxed beef report was modified to meet mandatory confidentiality criteria. We determined that the trend number could be calculated by the application if a modification was made to the application. MNB officials were aware of this and had requested changes to the LMPRS application about 2 years ago. Due to a change in personnel, the issue was never resolved. MNB supervisors explained that there was no second-party review because the reporters are considered the experts. MNB officials requested the application contractor determine what type of effort would be involved in making a program change to the trend calculation. However, the confidentiality data for the boxed beef report could not be handled by the application because parameters change frequently. During our fieldwork, MNB officials agreed that it was reasonable to pursue establishing procedures for second-party reviews of LMPRS reports.

Technical Documentation

While the technical system documentation for LMPRS is extensive, it did not provide a complete view of all files and database tables used within each module of the application. MNB did not have adequate internal controls requiring detailed technical documentation because they felt the documentation MNB requested of the contractor was adequate. In addition, MNB relied heavily on the current application contractor to provide technical information for the LMPRS application. There was a risk of system downtime if the current MNB application contractor was no longer available.

Departmental⁷ guidance states that agencies with new or significantly modified application systems should assure the development of adequate systems, program, operational, and user documentation and recognize⁸ the risk of a heavy reliance on contractors or other related parties to perform critical agency functions.

NIST guidance⁹ states documentation of all aspects of computer support and operations is important to ensure continuity and consistency. The guidance also states formalizing operational practices and procedures in sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

⁷ DM 3140-1, Management ADP Security Manual, Section 17 - Application System Development, dated July 19, 1984

⁸ DM 1110-2, Management Control Manual, Chapter 2, section 5 - Guidelines for Developing a Management Control Process, dated November 29, 2002

⁹ NIST SP800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 14, section 14.6, dated October 1995

The contractor provided a user guide for plant users and an administrator's guide for MNB users. There also is contractor-provided documentation for certain program functions used by the application and a high-level flowchart of the application. However, there is no comprehensive technical documentation that describes all of the application's tables and files including how transactions flow through the application. MNB felt that the original documentation requested from the contractor was sufficient. However, MNB officials have agreed that additional technical documentation should be obtained and stated the application contractor would be consulted on this issue.

Supervisory Reviews

MNB field office staff did not routinely perform supervisory reviews of MNB reporters' daily activities, and the reviews that were performed were not documented. MNB did not have adequate internal controls for review of MNB reporters' daily activities because supervisors did not believe it was necessary. There is an increased risk of errors occurring in the mandatory report process.

Federal guidance¹⁰ states internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations, that it is performed continually and is ingrained in the agency's operations, and that it includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

We interviewed supervisors and managers at the Des Moines field office. They stated that there was no documentation of, or consistent schedule for, supervisory reviews of the reporters' work, including transactions that are excluded from the mandatory LMPRS reports posted on the AMS website. The reporters submit a Daily Report Log, which summarizes the reporting activities each day, to supervisors. The Daily Report Logs contain the time of import of records, list of packers not submitting data and reason and percentage of records excluded, and the percent of records used in the reports. However, the supervisors do not routinely review the reporters' daily work that is summarized in the logs. MNB supervisors stated that the reporters were experts and that they trusted the reporters' judgment in making decisions.

Application Monitoring

MNB did not routinely monitor the daily operations of the application such as adequately reviewing database tables containing authorized users, firewall logs, and web server logs. MNB did not have adequate internal controls in place because officials were satisfied with their current monitoring activities.

¹⁰ GAO, Standards for Internal Control in the Federal Government, Monitoring Section, dated November 1999

Insufficient monitoring may increase the vulnerability of LMPRS to attacks, including inappropriate or unauthorized access and potential system downtime.

Federal guidance¹¹ states internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations, that it is performed continually and is ingrained in the agency's operations, and that it includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties. The guidance¹² also states management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs.

While the contractor monitors the firewall logs, MNB officials receive a summary of these logs daily, which contains the top threats and top threat sources for that day. MNB officials stated that they did not know much about the firewall logs. We obtained examples of the types of training the MNB IT staff had recently received; however, the list did not include any type of firewall training. MNB was not performing reviews of the authorized application users and web server access logs. The web server logs contain transaction data of submissions and retrievals of information from the application. The transactions that are recorded by these logs also can be used to monitor the date and time LMPRS users accessed the application. MNB officials stated they have routine meetings with the application contractor; however, there were no routine reviews of server logs. MNB officials did not have routine meetings with the other two contractors (firewall and facility).

Recommendation No. 1

Establish and implement application controls to ensure that LMPRS users are given only the access privileges required for assigned job duties.

Agency Response. AMS concurs with this recommendation. During the review, MNB staff modified the user access privileges to ensure that only those users whose job responsibilities require Administrator access have that privilege. No later than May 31, 2005, AMS will develop written procedures that will be incorporated in the Trusted Facilities Manual, developed during the certification and accreditation process, for MNB IT staff to follow when establishing new AMS and plant user accounts to ensure that Administrator access is given only to those users that require it.

¹¹ GAO, Standards for Internal Control in the Federal Government, Monitoring Section, dated November 1999

¹² GAO, Standards for Internal Control in the Federal Government, Managing Human Capital, dated November 1999

OIG Position. We accept the AMS management decision for Recommendation No. 1. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of the written procedures that have been developed to ensure that Administrator access is given only to AMS and plant user accounts that require it.

Recommendation No. 2

Determine all the mandatory reports that are modified before posting to the AMS website. For each report that is modified, (a) establish and implement application controls to ensure that the report is reviewed for correctness before being posted on the website, and (b) where possible, change the application to perform the needed functions.

Agency Response. AMS concurs with this recommendation. No later than May 31, 2005, MNB will determine all of the mandatory reports that are modified prior to being posted on the AMS website and will establish written procedures in an LMPRS reporter desk manual to ensure that all of the reports are subject to a second-party review by another reporter prior to publication. With respect to the reports that are being modified due to confidentiality concerns, AMS has determined that it is not possible to modify the application to perform this function. With respect to the swine reports in which a trend number is manually calculated, AMS will pursue modifying the application to perform this function in the next swine enhancement effort, which is anticipated to occur in fiscal year 2006.

On December 8, 2004, AMS provided correspondence with the following clarification: With respect to the AMS response to Recommendation No. 2, the swine reports that are modified to manually calculate the trend number will be subject to the second-party review procedures that AMS will establish, no later than May 31, 2005, until such time that the application is modified to perform this function.

OIG Position. We accept the AMS management decision for Recommendation No. 2. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of the written procedures that have been developed to ensure the correctness of modified reports.

Recommendation No. 3

Obtain necessary technical documentation for LMPRS.

Agency Response. AMS concurs with this recommendation. While AMS believes the current technical documentation for LMPRS is extensive, as a part of the contract that was awarded in September 2004 for the fiscal year 2004 enhancements, additional system documentation will be developed that details all of the application's tables and files, including how

transactions flow through the applications. This will be completed no later than May 31, 2005.

OIG Position. We accept the AMS management decision for Recommendation No. 3. In our opinion, final action will be completed when AMS provides OCFO/PAD evidence of the additional LMPRS documentation.

Recommendation No. 4

Establish and implement application controls for reviews of MNB reporters' activities, including documentation of the reviews.

Agency Response. AMS concurs with this recommendation. No later than May 31, 2005, MNB will develop procedures to be incorporated in the LMPRS reporter desk manual to document weekly reviews of MNB reporters' activities, including transactions that were excluded from the LMPRS reports, by the appropriate supervisor(s).

OIG Position. We accept the AMS management decision for Recommendation No. 4. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of the written procedures that have been developed to ensure supervisory reviews of MNB reporters' activities are performed and documented.

Recommendation No. 5

Establish and implement application controls for review of the daily operations of the LMPRS application.

Agency Response. AMS concurs with this recommendation. No later than May 31, 2005, AMS will establish and implement controls to review the daily operations of the LMPRS application. As a part of the contract that was awarded in September 2004 for the fiscal year 2004 enhancements, the LMPRS application will generate a nightly audit report that will include items such as the number of imports run (including details for each import), total LMPRS records processed, total LMPRS bad records detected, the number of reports run (including details for each report), user account details, and other application information.

OIG Position. We accept the AMS management decision for Recommendation No. 5. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of the written procedures that have been developed to review the daily operations of the LMPRS application.

Recommendation No. 6

Establish and implement application controls to ensure that the appropriate personnel receive adequate training to monitor the LMPRS application.

Agency Response. AMS concurs with this recommendation. AMS has outsourced both the overall administration of the system, including management of the system firewalls, to third-party contractors. AMS believes these contractors have the qualifications and skills necessary to effectively carry out these tasks. In the event that additional expertise is needed to review either firewall logs or other system functions, agency IT personnel are available to MNB for consultation as needed. If AMS believes further training is needed for overall program management, AMS will pursue obtaining additional training as appropriate.

OIG Position. We accept the AMS management decision for Recommendation No. 6. The proposed actions, in our opinion, are sufficient for final action.

Section 2 Management Controls Need Improvement

Finding 2 Information System Documentation and Policies Need Improvement

Our review of the LMPRS application disclosed several conditions that were not in accordance with Federal and Departmental guidance. The security plan did not address all requirements. MNB did not submit Plan of Action and Milestones (POA&M) data to address LMPRS application weaknesses. MNB had not certified the LMPRS application or performed scans of the LMPRS network for system vulnerabilities. The cause of the conditions was that AMS had inadequate management controls to ensure Federal and Departmental guidance was followed, as outlined in the sections below. As a result, the LMPRS application could be vulnerable to security breaches and cyber-related attacks.

Security Plan

The LMPRS security plan did not address all Federal and Departmental requirements including waivers for noncompliance with policies requiring warning banner displays, user password expiration, and locking out of administrator accounts on the LMPRS servers. In addition, the security plan did not indicate the current status of all elements outlined in the security plan guidance. AMS' CIO had not informed MNB of the requirements outlined in the guidance. Thus, MNB officials were not aware of all the requirements outlined by the guidance. As a result, the LMPRS application could be vulnerable to security breaches.

Federal guidance¹³ states that all major applications and general support systems containing sensitive information require protection to assure their integrity, availability, or confidentiality, and therefore require security plans. Departmental guidance requires warning¹⁴ banners, password¹⁵ expiration, and locking out of user accounts.¹⁶ Further,¹⁷ when it is not feasible to apply a particular standard to an existing automated data processing (ADP) system without excessive costs, agencies are to devise an alternate scheme for adequate protection and then request a waiver. Office of the Chief Information Officer (OCIO) guidance¹⁸ also requires the security plan to discuss upcoming agency plans for implementing the agency security awareness, training, and education programs including planned annual

¹³ OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," section A, dated November 28, 2000

¹⁴ Departmental Regulation 3140-1, USDA Information Systems Security Policy, Section 15 - System Warning Message, dated May 15, 1996

¹⁵ DM 3140-1, Management ADP Security Manual, Appendix D, section 6, part b, dated July 19, 1984

¹⁶ DM 3140-1, Management ADP Security Manual, Appendix D, section 5 - Requirements, dated July 19, 1984

¹⁷ DM 3140-1, Management ADP Security Manual, Section 7 - Security Program Requirements, dated July 19, 1984

¹⁸ OCIO Cyber Security (CS)-25, Annual Agency Security Plans for Information Technology Systems and Security Programs Guidance, dated April 8, 2003

security seminars. The Departmental OCIO's office issued a letter¹⁹ stating annual security plans are recognized as one tool to assess and report on the protection of agency assets. Therefore, it is critical that they be prepared/updated on a regular basis with the most current information concerning each agency's information security practices.

The most recent LMPRS security plan, dated January 6, 2004, stated, "The LMPRS does not display banners or legal notices prior to the display of the logon dialog box. Implementing this would require an administrator to physically click 'ok' to get past the desktop, which would prevent certain critical applications in the startup group not to start without a manual interface. Servers are set up to automatically reboot periodically, implementing the above requirement would impact this job." The security plan also stated that LMPRS user passwords did not expire. In addition, the security plan stated, "There is currently no lockout feature in place for the LMPRS servers. All accounts belong to the administrator group, and therefore cannot be locked out or disabled." When asked about the above-mentioned requirements, MNB responded that it was not aware that waivers were required for conditions that did not comply with security plan guidance until notified by OIG during our fieldwork. During our fieldwork, MNB modified the application to display warning banners, and has initiated changes to the application to resolve the password expiration issue. MNB stated it would pursue getting a waiver for the locking out of the system administrator accounts from OCIO and also discuss the need to have the system administrator accounts lock out.

The LMPRS security plan did not include the frequency of security training, as required by the OCIO guidance stated above. MNB stated that there was annual security training for personnel as well as training on the LMPRS application before using the application, even though it was not noted in the security plan. Also, the wording in the security plan did not always indicate the current status of the element being reported on. For instance, the word "should" used in the Rules of Behavior section does not indicate if the rules are being used.

Plan of Action and Milestones

MNB did not prepare and submit POA&M data to address identified weaknesses in the LMPRS application. The AMS CIO had not informed MNB of the requirements outlined in the Federal guidance. Thus, MNB officials were not aware of all the requirements outlined by the Federal²⁰ guidance. The LMPRS application could be vulnerable to any weaknesses that have been identified in risk assessments, network vulnerability scans, and audit reports.

¹⁹ OCIO Letter, Annual Agency Security Plans for Information Technology Systems and Security Programs, dated April 28, 2003

²⁰ OMB, Memorandum for the Heads of Executive Departments and Agencies, M-02-01, dated October 17, 2001

Federal guidance²¹ states, “An agency should develop a separate POA&M for every program and system for which weaknesses were identified * * *.” The guidance further states, “Thereafter, brief status updates must be submitted on a quarterly basis.”

MNB was not aware of the submission requirements for a POA&M until notified by OIG during our fieldwork. The AMS CIO stated that his office was responsible for preparing the POA&M for the agency and that each branch was responsible for reporting vulnerabilities. We obtained a copy of the most recent POA&M submissions from the AMS CIO. There were no submissions from MNB. Although AMS’ CIO did not make it a practice to send out specific communications on Departmental requirements because of the workload and loss of staff, the AMS CIO’s office was available to consult with the branches.

Since the LMPRS vulnerabilities from a recent risk assessment were not “high” risk, MNB made the decision to include the complete POA&M in the planned certification and accreditation process due in September 2004. The AMS CIO stated that his office formed a new Cyber Security Branch in June 2004 that will be more involved with each of the AMS program areas.

Certification and Accreditation

The LMPRS application had not been certified and accredited. MNB did not follow Federal and Departmental guidance requiring certification and accreditation when the application went into production in April 2001 and had not pursued the matter since. As a result, the LMPRS application could be vulnerable to security breaches and cyber-related attacks.

Departmental guidance²² states the need for certification is recognized by the OMB²³ and that Federal agencies are required to certify the security of sensitive computer application systems and perform recertification at least every 3 years.

MNB officials stated that when the LMPRS went into production in April 2001, the certification and accreditation process was not adhered to on a Departmental level. The Department has set September 2004 as the date for certifications to be completed, and MNB stated that the LMPRS certification process should be completed before September 2004. The AMS CIO agreed with the branch’s assessment that the Department had not been adhering to the certification requirements in the past. The CIO stated that Federal guidance had not been in place for the process and had been recently developed. The AMS CIO also stated that his office formed a new Cyber Security Branch in June 2004 that will be more involved with each of the AMS program areas.

²¹ OMB, Memorandum for the Heads of Executive Departments and Agencies, M-02-01, dated October 17, 2001

²² DM 3140-1, Management ADP Security Manual, Section 12 - Application Certification and Recertification, dated July 19, 1984

²³ OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources,” General Support Systems, dated November 28, 2000

Network Scans

The current LMPRS network was not being scanned at the time of our fieldwork. MNB had no formal policies and procedures in place to ensure network scans are completed and corrective actions are taken on vulnerabilities identified on the LMPRS network due to an oversight by officials. As a result, LMPRS servers and networks could be vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of the data compiled on tracking and reporting livestock data.

OMB Circular A-130²⁴ requires agencies to maintain security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls. Departmental guidance²⁵ requires agencies to keep an inventory of their network, to perform monthly network scans, and to develop and implement corrective action plans to address critical vulnerabilities. Federal guidance²⁶ also states that contractors are held to the same security standards as Government entities.

We used a commercially available software tool that identifies vulnerabilities in network components that use the Transmission Control Protocol/Internet Protocol (the protocol used on the public Internet). We found one medium-risk and no high-risk vulnerabilities on LMPRS network routers, switches, and servers. The medium-risk vulnerability was a software analysis function that was enabled and could be exploited. Sensitive system information could be obtained and used to further attack the servers.

MNB officials stated that they did not realize that they needed to (1) scan servers before placing the servers on the network, (2) include IP addresses for routers and switches in the scanning process, and (3) develop corrective action plans to address identified vulnerabilities. In a prior audit,²⁷ we reported that network scans were not being performed. The officials stated the internal servers that were not part of LMPRS were being scanned regularly as a result of the prior audit. The MNB official stated that because the LMPRS servers are outside the USDA network (see diagram on page 2) that they were overlooked. The AMS CIO stated that he was not aware that scans of the LMPRS network were not being performed and told the appropriate staff that all AMS servers should be scanned including those external to the USDA network. During the audit fieldwork, MNB started

²⁴ OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," section A, dated November 28, 2000

²⁵ DM 3500-2, Cyber Security Manual, Chapter 6, part 1, dated April 4, 2003

²⁶ Federal Information Security Management Act of 2002, dated December 17, 2002

²⁷ Audit Report No. 10099-1-FM, "Security Over Information Technology Resources at the Agricultural Marketing Service," dated March 2002

performing monthly scans of the LMPRS servers and plans to add scans of the switches and routers soon. Due to our audit work, AMS became aware that the facility contractor had a process in place for identifying and mitigating network vulnerabilities; however, assurance of this fact was not mentioned in the statement of work or contract for hosting the LMPRS system. The AMS CIO stated that his office formed a new Cyber Security Branch in June 2004 that will be more involved with each of the AMS program areas.

Recommendation No. 7

Establish and implement management controls to ensure that the LMPRS security plan conforms to Federal and Departmental regulations, including the requirement that appropriate waivers for existing and future LMPRS noncompliant conditions are requested and each area of the plan is completely addressed.

Agency Response. AMS concurs with this recommendation. MNB will work with the newly establish Cyber Security Branch to ensure that the LMPRS security plan conforms to Federal and Departmental regulations, including appropriate waivers for noncompliant conditions. No later than May 31, 2005, MNB and the Cyber Security Branch will ensure that the LMPRS security plan is updated as appropriate. On December 13, 2004, AMS provided correspondence with the following clarification: Further, no later than September 2005, management controls will be established and implemented to ensure future security plans conform with Federal and Departmental regulations.

OIG Position. We accept the AMS management decision for Recommendation No. 7. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of management controls to ensure that the LMPRS security plan conforms to Federal and Departmental regulations, including an updated LMPRS security plan.

Recommendation No. 8

Establish and implement management controls to ensure POA&M data is compiled and updated as required for LMPRS.

Agency Response. AMS concurs with this recommendation. MNB and Cyber Security Branch staff will ensure a POA&M is completed for the LMPRS by January 31, 2005. On December 13, 2004, AMS provided correspondence with the following clarification: Further, no later than September 2005, management controls will be established to ensure that POA&M data will be routinely updated in the future.

OIG Position. We accept the AMS management decision for Recommendation No. 8. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of a completed POA&M that includes LMPRS data.

Recommendation No. 9

Establish and implement management controls to ensure that the appropriate agency personnel are aware of Departmental requirements for information security, including security plans, POA&M data, and network scans.

Agency Response. AMS concurs with this recommendation. AMS will supplement Departmental guidance with written agency directives regarding the use of system security plans, network patching and scanning, and POA&M reporting by September 2005.

OIG Position. We accept the AMS management decision for Recommendation No. 9. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of the written agency directives for system security plans, network patching and scanning, and POA&M reporting.

Recommendation No. 10

Establish and implement management controls for the certification, accreditation, and periodic recertification of the LMPRS application.

Agency Response. AMS concurs with this recommendation. The LMPRS application was certified and accredited on September 9, 2004. AMS will ensure that the LMPRS application is recertified as required by Federal and Departmental guidance. On December 13, 2004, AMS provided correspondence with the following clarification: Further, no later than September 2005, management controls will be established and implemented to ensure the LMPRS application will be recertified as required by Federal and Departmental guidance.

OIG Position. We accept the AMS management decision for Recommendation No. 10. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation that the LMPRS application has been certified and accredited.

Recommendation No. 11

Establish and implement management controls to perform monthly network scans of LMPRS and develop corrective action plans for critical vulnerabilities.

Agency Response. AMS concurs with this recommendation. MNB began monthly scans of the LMPRS network during the OIG review. Any critical vulnerability that is identified is provided to the contractor for appropriate mitigation. Any corrective action taken (e.g., security patches) is documented in the system documentation. No later than May 31, 2005, the Trusted Facilities Manual will be modified to include the procedures for performing scans and addressing any corrective action required.

OIG Position. We accept the AMS management decision for Recommendation No. 11. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation of the written procedures for performing scans and addressing any corrective action required.

Recommendation No. 12

Establish and implement management controls to ensure contracts with service organizations include coverage of vulnerability identification and mitigation, such as router scans.

Agency Response. AMS concurs with this recommendation. The only AMS service agreement that involves contractor support for vulnerability identification and mitigation is the LMPRS agreement. MNB will modify the LMPRS service agreement upon its renewal in September 2005 to specify vulnerability identification and mitigation services. On December 13, 2004, AMS provided correspondence with the following clarification: Further, no later than September 2005, management controls will be established and implemented to ensure that any future contracts will include coverage of vulnerability and mitigation.

OIG Position. We accept the AMS management decision for Recommendation No. 12. In our opinion, final action will be completed when AMS provides OCFO/PAD documentation that the LMPRS contract has been modified to include vulnerability identification and mitigation services.

General Comments

We determined that the operations of two of the four LMPRS contractors have had some level of review by a third party. Professional auditing standards²⁸ state that when a user organization uses a service organization, transactions that affect the user organization's financial statements are subjected to controls that are, at least in part, physically and operationally separate from the user organization. Service organizations include bank trust departments that invest and service assets for employee benefit plans or for others, mortgage bankers that service mortgages for others, and application service providers that provide packaged software applications, and a technology environment that enables customers to process financial and operational transactions.

External users of the LMPRS application rely on the data for financial decisions such as the purchase and sale of livestock. Therefore, we believe that it would be prudent for MNB to require reviews for the LMPRS contractors, which are conducted based on the above-mentioned professional auditing standards.

²⁸ American Institute of Certified Public Accountants Professional Standards, AU Section 324: Service Organizations, as amended by applicable statements on auditing standards

Scope and Methodology

Our audit was part of a nationwide audit of selected USDA agencies. We selected AMS' LMPRS application from a listing submitted in November 2003 by USDA agencies of their major applications and general support systems needing to be certified and accredited by September 2004 to OCIO. The application was chosen based on it being mission critical and our knowledge of previous agency audits. The Livestock and Grain MNB Headquarters is in Washington, D.C., and the two field offices that handle mandatory information are in Des Moines, Iowa, and St. Joseph, Missouri. There are approximately 134 plants that submit mandatory data to the LMPRS application. We performed audit work at the AMS MNB located in Washington, D.C., and the AMS Des Moines Field Office in Des Moines, Iowa. We also visited the application contractor, who developed and maintains the application for AMS, and four judgmentally selected plants. We reviewed the AMS LMPRS activities for fiscal year 2004 and other years as necessary to develop the findings. We selected transactions made during the period from October 1 to October 24, 2003, comprised of data from 115 of the 134 plants. We selected 4 of the 115 plants to visit. Our fieldwork was performed during and for the period January 2004 through July 2004.

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

- We interviewed responsible agency and contractor officials managing the application system, as well as both agency and plant users of the system.
- We reviewed, tested, and compared LMPRS application policies, procedures, handbooks, and administrative records to the requirements of Federal regulations, Departmental regulations, and other sources.
- We judgmentally selected 4 of 115 plants to examine controls over source documents and submission of LMPRS mandatory information. The plant selections were based on the method of data submission and proximity to the OIG Southwest Regional Office and the AMS Des Moines Field Office. The controls we examined included authorization, data terminal security, and accuracy of the data submissions. We verified a sample of transaction data submitted by each of the four plants.
- We performed Transmission Control Protocol/Internet Protocol vulnerability scans on various LMPRS network components.

This audit was conducted in accordance with generally accepted Government auditing standards. Therefore, the audit included tests of program and accounting records considered necessary to meet the audit objectives.

Exhibit A – Agency Response

Exhibit A – Page 1 of 5

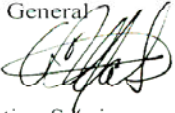


United States
Department of
Agriculture

Agricultural
Marketing
Service

1400 Independence Avenue, SW
Room 3529-S, STOP 0203
Washington, DC 20250-0203

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

FROM: A. J. Yates 
Administrator
Agricultural Marketing Service

December 1, 2004

SUBJECT: Livestock Mandatory Price Reporting System – Application Controls
Audit 01099-4-Te

We have reviewed the subject audit report and agree in principle with the findings and recommendations. Our detailed response, including actions already taken and actions to be taken to address the recommendations, is attached.

If you have any questions or need further information, please contact Neil Blevins, our Management Control Officer, at 202-720-6766.

Attachment

**Agricultural Marketing Service Responses
To OIG Inspection Recommendations
Audit 01099-4-Te**

Recommendation No. 1

Establish and implement application controls to ensure that LMPRS users are given only the access privileges required for assigned job duties.

Agency Response: During the review, Livestock and Grain Market News (MNB) staff modified the user access privileges to ensure that only those users whose job responsibilities require Administrator access have that privilege. No later than May 31, 2005, AMS will develop written procedures that will be incorporated in the Trusted Facilities Manual (TFM), developed during the certification and accreditation process, for MNB IT staff to follow when establishing new AMS and plant user accounts to ensure that Administrator access is given only to those users that require it.

Recommendation No. 2

Determine all the mandatory reports that are modified before being posted on the AMS website. For each report that is modified, (a) establish and implement application controls to ensure that the report is reviewed for correctness before being posted on the website, and (b) where possible, change the application to perform the needed functions.

Agency Response: No later than May 31, 2005, MNB will determine all of the mandatory reports that are modified prior to being posted on the AMS website and will establish written procedures in a LMPRS reporter desk manual to ensure that all of the reports are subject to a second-party review by another reporter prior to publication. With respect to the reports that are being modified due to confidentiality concerns, AMS has determined that it is not possible to modify the application to perform this function. With respect to the swine reports in which a trend number is manually calculated, AMS will pursue modifying the application to perform this function in the next swine enhancement effort, which is anticipated to occur in FY06.

Recommendation No. 3

Obtain adequate technical documentation for LMPRS from the contractor.

Agency Response: While AMS believes the current technical documentation for LMPRS is extensive, as part of the contract that was awarded in September 2004 for the FY04 enhancements, additional system documentation will be developed that details all of the application's tables and files, including how transactions flow through the application. This will be completed no later than May 31, 2005.

Recommendation No. 4

Establish and implement application controls for routine reviews of MNB reporters' activities, including documentation of the reviews.

Agency Response: No later than May 31, 2005, MNB will develop procedures to be incorporated in the LMPRS reporter desk manual to document weekly reviews of MNB reporters' activities, including transactions that were excluded from the LMPRS reports, by the appropriate supervisor(s).

Recommendation No. 5

Establish and implement application controls for review of the daily operations of the LMPRS application.

Agency Response: No later than May 31, 2005, AMS will establish and implement controls to review the daily operations of the LMPRS application. As part of the contract that was awarded in September 2004 for the FY04 enhancements, the LMPRS application will generate a nightly audit report that will include items such as the number of imports run (including details for each import), total LMPRS records processed, total LMPRS bad records detected, the number of reports run including details for each report, user account details and other application information.

Recommendation No. 6

Establish and implement application controls to ensure that the appropriate personnel receive adequate training to monitor the LMPRS application.

Agency Response: AMS has outsourced both the overall administration of the system, including management of the system firewalls, to third-party contractors. AMS believes these contractors have the qualifications and skills necessary to effectively carry out these tasks. In the event that additional expertise is needed to review either firewall logs or other system functions, Agency IT personnel are available to MNB for consultation as needed. If AMS believes further training is needed for overall program management, AMS will pursue obtaining additional training as appropriate.

Recommendation No. 7

Establish and implement management controls to ensure that the LMPRS security plan conforms to Federal and Departmental regulations, including that appropriate waivers for existing and future LMPRS noncompliant conditions are requested and each area of the plan is completely addressed.

Agency Response: MNB will work with the newly established Cyber Security Branch (CSB) to ensure that the LMPRS security plan conforms to Federal and Departmental regulations, including appropriate waivers for noncompliant conditions. No later than May 31, 2005, MNB and CSB will ensure that the LMPRS security plan is updated as appropriate.

Recommendation No. 8

Establish and implement management controls to ensure POA&M data is compiled and routinely updated for LMPRS.

Agency Response: MNB and CSB staff will ensure that a POA&M is completed for the LMPRS application by January 31, 2005.

Recommendation No. 9

In consultation with the AMS CIO, establish and implement management controls to ensure that the appropriate Agency personnel are aware of Departmental requirements for information security including security plans, POA&M data, and network scans.

Agency Response: AMS will supplement Departmental guidance with written agency directives regarding the use of system security plans, network patching and scanning, and POA&M reporting by September 2005.

Recommendation No. 10

Establish and implement management controls for the certification and periodic recertification of the LMPRS application.

Agency Response: The LMPRS application was certified and accredited on September 9, 2004. AMS will ensure that the LMPRS application is recertified as required by Federal and Departmental guidance.

Recommendation No. 11

Establish and implement management controls to perform monthly scans of LMPRS and develop corrective action plans for critical vulnerabilities.

Agency Response: MNB began monthly scans of the LMPRS network during the OIG review. Any critical vulnerability that is identified is provided to contractor for appropriate mitigation. Any corrective action taken (e.g., security patches) is documented in the system documentation. No later than May 31, 2005, the TFM will be modified to include the procedures for performing scans and addressing any corrective action required.

Recommendation No. 12

Establish and implement management controls to ensure contracts with service organizations include coverage of vulnerability identification and mitigation, such as router scans.

Agency Response: The only AMS service agreement that involves contractor support for vulnerability identification and mitigation is the LMPRS agreement. MNB will modify the LMPRS service agreement upon its renewal in September 2005 to specify vulnerability identification and mitigation services.