



U.S. Department of Agriculture



Office of Inspector General
Great Plains Region

Audit Report

Farm Service Agency Price Support Loan Application

Report No. 03099-195-KC
September 2005



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20250



DATE: September 30, 2005

REPLY TO
ATTN OF: 03099-195-KC

TO: James R. Little
Administrator
Farm Service Agency

ATTN: T. Mike McCann
Director
Operations and Review Analysis Staff

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

SUBJECT: Farm Service Agency Price Support Loan Application

This report presents the results of our audit of the Farm Service Agency Price Support Loan Application. Your response to the draft report, dated August 1, 2005, is included in its entirety as exhibit A with excerpts and the Office of Inspector General's position incorporated into the relevant sections of the report. We made editorial changes, where needed, based upon your written comments.

We agree with your management decisions for Recommendations 1, 2, 3, 4, and 6. Please follow your agency's internal procedures in forwarding final action to the Office of the Chief Financial Officer. Final action on the management decisions should be completed within 1 year of the date of this report to preclude being listed in the Department's Performance and Accountability Report.

For Recommendation 5, management decision is contingent upon the pending Office of the Chief Information Officer's decision regarding the waiver of Departmental requirements. If a waiver is not granted, then a corrective action plan will be needed regarding data transmission for the specific service centers. For Recommendation 7, additional information is needed on the actual or anticipated timeframe the updated contingency plan instructions were provided to the county offices and the identified procedures to provide oversight of the plans. In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective action taken, or planned, and the timeframes for implementation for Recommendations 5 and 7. Please note that the regulation requires a management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

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

Executive Summary

Farm Service Agency Price Support Loan Application (Audit Report No. 03099-195-KC)

Results in Brief

This report presents the results of our audit of the price support loan application within the Farm Service Agency's (FSA) Automated Price Support System (APSS). Our overall objective was to assess whether the FSA had adequate management, security, and programming controls over its price support loan application. The FSA relies on the APSS to make and service commodity loans and loan deficiency payments, a critical function of the Commodity Credit Corporation's mission to stabilize, support, and protect farm income and prices.

Overall, we found that FSA had generally implemented sufficient controls to ensure the integrity of the price support loan application system. However, our audit identified areas where improvements were warranted regarding application programming, access, and security. Specifically, we found that:

- weaknesses existed in several automated checks used to validate data in the price support loan application;
- controls over logical access, including passwords to its price support loan application, did not assure adherence to federal guidance because employees were required to divulge their passwords, and password intervals were not properly set;
- a lack of controls existed over transmission of data without the appropriate security measures;
- incomplete risk assessment documentation existed for the price support loan application; and
- contingency plans did not describe the expected recovery actions to be taken by county offices.

Recommendations In Brief

We recommend that the FSA:

- conduct a detailed analysis of the adequacy of the key validation controls for the price support application;
- develop and document validation controls to mitigate the specific weaknesses determined;

- revise FSA direction on logical access control guidance to be consistent with Departmental requirements;
- ensure that employees who have made their passwords and user identifications available to others obtain passwords and user identifications in accordance with Departmental security guidance;
- consult with Office of the Chief Information Officer (OCIO) and implement adequate security to ensure that all sensitive data is transmitted securely in accordance with applicable requirements;
- conduct sufficient reviews of risk assessments to establish that all relevant information has been documented and considered as part of the assessment's development (e.g., network topology, list of system personnel, and connected applications) prior to acceptance of the work and payment; and
- revise contingency plans for county offices that will provide the achievable processes to be followed for continued operation if an emergency arises and establish oversight of the plans.

FSA Response

In its August 1, 2005, written response to the draft report, FSA concurred with the findings and recommendations in the report, and provided timeframes for completing many of corrective actions.

OIG Position

We agree with management decision for Recommendations 1, 2, 3, 4, and 6. The management decision for Recommendation 5 is contingent upon the pending Office of the Chief Information Officer decision regarding the waiver of Departmental requirements. If a waiver is not granted, then a corrective action plan and applicable timeframes are needed. For Recommendation 7, additional clarification is needed on when the updated contingency plan instructions will be provided to county offices and the procedures to provide oversight of the plans to ensure that they accurately describe expected actions.

Abbreviations Used in This Report

ADP	Automated Data Processing
APSS	Automated Price Support System
C&A	Certification and Accreditation
CCC	Commodity Credit Corporation
CS	Cyber Security
DM	Departmental Manual
DR	Departmental Regulation
FSA	Farm Service Agency
ID	Identification
IT	Information Technology
ITS	Information Technology Services
ITSD	Information Technology Services Division
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PSD	Price Support Division
RA	Risk Assessment
USDA	United States Department of Agriculture

Table of Contents

Executive Summary	i
Background and Objectives	1
Findings and Recommendations	3
Section 1 Application Programming	3
Finding 1 FSA Lacks Assurance that Price Support Loan Application is Correctly Programmed to Validate Data.....	3
Recommendation 1	4
Recommendation 2	5
Section 2. Application Access	7
Finding 2 Logical Access Controls Security Needs Strengthening	7
Recommendation 3	8
Recommendation 4	9
Finding 3 Remote Access Security Needs Strengthening	9
Recommendation 5	10
Section 3. Documentation	12
Finding 4 Inadequate Risk Assessment Documentation	12
Recommendation 6	13
Finding 5 Contingency Plans Need Revision	13
Recommendation 7	14
Scope and Methodology	16
Exhibit A – FSA Response	17

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 by the computer.

Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer. In addition, general security controls and automated controls built into the operating system that support the application should also be considered. Weak controls that allow physical or logical access to the computers that store application data could be used to circumvent the controls established within the application itself.

The Commodity Credit Corporation (CCC) is a Government owned corporation created in 1933 to stabilize, support, and protect farm income and prices; to help maintain balanced and adequate supplies of agricultural commodities, including products, foods, feeds, and fibers; and to help in the orderly distribution of these commodities. Management of the CCC is vested in a board of directors, subject to the general supervision and direction of the Secretary of Agriculture. The activities of the CCC are carried out mainly by the personnel and through the facilities of the Farm Service Agency (FSA) and its State and county committees. There are 51 FSA State offices and about 2,500 U.S. Department of Agriculture (USDA) Service Centers. Additionally, the FSA maintains field office personnel in Kansas City and St. Louis, Missouri, and Salt Lake City, Utah.

Various laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974, the Federal Information Security Management Act of 2002, and the Paperwork Reduction Act of 1995. Departmental responsibilities were recently reemphasized in the Clinger-Cohen Act of 1996 and Presidential Decision Directive 63, "Policy on Critical Infrastructure Protection." Additionally, the Government Information Security Reform Act was enacted on October 30, 2000. This Act codified the existing requirements of the Office of Management and Budget's (OMB)

Circular A-130, Appendix III, Security of Federal Automated Information Resources. Computer security at USDA is addressed in Departmental Manual (DM) 3140-1, Management Automated Data Processing (ADP) Security Manual, and various Departmental Regulations (DR). Additionally, the FSA has issued certain security guidelines in a series of IRM Handbooks.

FSA uses a software application called the Automated Price Support System (APSS) to carryout the CCC marketing assistance loan program. The price support loan application is software within the APSS that facilitates marketing assistance loans provided to producers at harvest time, or after, to meet cash flow needs without having to sell their commodities when market prices are typically at harvest-time lows. Marketing loans allow producers to store production at harvest facilities and market their commodities throughout the year. Marketing assistance loans for covered commodities are pledged as loan collateral, and producers have the option of delivering the pledged collateral to the CCC as full payment for the loan at maturity. Market loan repayment provisions specify, under certain circumstances, that producers may repay loans at less than principal plus accrued interest and other charges. For crop year 2002, FSA/CCC processed 176,000 loans that totaled about \$7.5 billion.

The APSS was developed to completely record county office data for the marketing loan assistance and loan deficiency payments made to producers. The APSS is comprised of a distributed data processing system that provides field offices the capability to make and service commodity loans and loan deficiency payments and a reporting and accounting feeder system that provides centralized tracking of all loan detail (transactions) and summary reporting capabilities. The price support loan application calculates the commodity loans, prepares loan documents and disbursements, provides for repayments, transfers, forfeitures, settlements, establishes receivables, and calculates interest charges. The system interfaces with accounting, inventory and production adjustment applications, and summarized data files are transmitted from the county and State offices on a daily or weekly basis for use in preparation of national level reports.

The USDA Office of Inspector General (OIG), conducted nationwide audits of selected USDA agencies to assess overall application controls of their computer systems to ensure the confidentiality, integrity, and availability of information. The FSA was one of the agencies selected for review.

Objectives

The objective of this audit was to determine if FSA had adequate management, security, and programming control over its price support loan application.

Findings and Recommendations

Section 1 Application Programming

Finding 1

FSA Lacks Assurance that Price Support Loan Application is Correctly Programmed to Validate Data

The price support loan application lacks several automatic checks to validate critical information that is used to make loan decisions. For example, the application should filter out loan requests that are made after the final date that a loan is available, but our testing showed it would allow loans to be made up to 2 months after this date has passed. However, we were unable to determine why these checks have not been incorporated into the application because FSA has not adequately recorded and retained documentation showing the changes it has made to the system through the years and FSA officials could not otherwise provide any information to explain the omissions. The application may have lacked these checks in its original programming, or the agency may have removed the checks in subsequent updates. In either case, without documentation tracking the history of changes made to the application, the agency cannot be assured that changes made to the system are authorized and accurate.

Federal standards mandate that data within computer systems must be validated continuously, which involves determining if it is accurate, complete, consistent, and reasonable (Federal Information Processing Standards 73). To accomplish this goal, agencies incorporate automatic validation controls that restrict users from entering predictably invalid data (e.g., wrong State codes), changing critical data (e.g., Federal loan interest rates), superceding established timeframes (e.g., submitting a loan request past the due date), and so on.

As users discover validation weaknesses in an application, agencies update the automatic controls to fix the problem. DM 3200-001 holds that changes made to major applications should be maintained throughout the life cycle of that system. Chapter 1.6 calls complete and accurate documentation of major application systems “essential.” More specifically, chapter 2.8 requires that managers maintain documentation related to the development, operation, and maintenance of an application throughout its use by an agency. DM 3200-002 also requires agencies to document software changes.

Our tests determined several validation weaknesses in FSA's price support loan application. In our tests at the FSA test site, the application:

- Accepted crop loans 2 months after the final loan availability date for a given crop,
- Permitted users to change interest rate tables, established yield tables, and service fees, which are critical to determining loan parameters,
- Prevented users from entering accurate information (e.g., test crop weights ending in 50 were not accepted by the system). For example, while entering a loan, a test weight of 250 was entered but the computer would not accept this number so a test weight of 300 was entered and accepted by the system. We tested various test weight numbers in increments of "50" (i.e., 150, 250, 350, etc) and found these would not be accepted by the system.
- Changed information input by the user (e.g., an entry of 2.56 bushels per acre was changed to 3156, and 'K' entered as a response to a yes (Y) or no (N) question was taken as a no (N)), and
- Allowed inaccurate State codes to be entered.

Proposed changes to FSA's price support loan application go through an appropriately rigorous process of development and testing before they are implemented throughout the agency. The agency, though, has not kept track of all the changes that it has made to validation controls. It also has not compiled the updates as they are released. This lack of documentation may lead to the agency undoing preceding programming changes designed to enhance the validation controls within the application. Any or all of the weaknesses identified above, for example, may have developed from conflicts between programming changes. Alternately, implemented validation controls may have been incorrectly removed if an older software update was re-released, in effect returning the application to an earlier, less effective version. The correction of these individual weaknesses could enhance the overall strength of the application's automatic validation control.

Recommendation 1

Conduct a detailed analysis of the adequacy of the key validation controls for the price support application.

Recommendation 2

Develop and document validation controls to mitigate the specific weaknesses cited above and those identified during the detailed analysis.

FSA Response.

In its August 1, 2005, response, FSA concurred with Recommendations 1 and 2, and the Price Support Division (PSD) conducted a preliminary detailed review and analysis specific to the weaknesses addressed in Finding 1. Of the weaknesses cited, PSD developed a validation control to accept a marketing assistance loan application within the final loan availability period applicable to the crop. This software enhancement will be released in county Release 568 and was scheduled to be released on July 25, 2005.

PSD analysis found one screen where the alpha, other than “Y” or “N” was permitted to a question requiring a yes or no response. PSD will issue a user requirement to request an enhancement to this validation. The user requirement will be completed by August 31, 2005.

FSA also stated that they found through their analysis that APSS does not validate against test weight that is not applicable to a specific commodity.

Human interaction is required for the remaining weaknesses cited in the audit which make an automated validation impossible. However, PSD will issue a directive to the State and county offices reminding them of the procedure for maintaining table files and to ensure program validations are correctly applied.

FSA is in the beginning stages to develop a web based eLOAN application process via the internet. When this is completed, the APSS will not be needed to support marketing assistance loans. The user requirement was issued to address this project on June 26, 2005. A more in-depth validation system will be implemented with this process in all activities pertaining to all programs currently used by APSS.

Because all resources are assigned to the eGOV initiatives, any additional enhancements in APSS may be prohibited, as directed by FSA Administration and the Information Technology Services Division (ITSD). However, FSA will make every attempt to ensure that validations remain a top priority in development of software. FSA's

response shows that the target date for completing final action is August 31, 2005.

OIG Position.

We clarified what information was tested in the bullet shown above regarding test weight numbers in increments of “50” (150, 250, 350) and performed additional testing for corn and wheat using a test weight of 50. We found that the APSS should not and does not allow a 50 test weight for wheat in all grades (1-5) and correctly does allow a 50 test weight for corn. Therefore, we accept management decision for Recommendations 1 and 2. For final action, FSA will need to report to the Office of the Chief Financial Officer (OCFO) that the proposed actions have been accomplished.

Section 2. Application Access

Finding 2

Logical Access Controls Security Needs Strengthening

FSA does not have adequate control over logical access to its price support loan application.¹ FSA direction inappropriately requires employees to divulge their passwords to other employees, and systems are not set to adequately restrict access. With loose control over passwords and protective steps not taken, the price support loan application becomes vulnerable to unauthorized use and FSA becomes less capable of establishing accountability for that misuse.

According to National Institute of Standards and Technology (NIST) 800-12, if passwords are used for authentication, organizations should teach users not to use easy-to-guess passwords, not to divulge their passwords, and not to store passwords where others can find them.²

Counter to these requirements, agency, State, and county guidance direct employees to make their passwords available to other employees for administrative purposes. FSA's handbook of computer operations directs field offices to print and store user identifications and passwords.³ Also,

- a State office notice required all county offices in a State to send master security user identifications (ID) and passwords to the State office.⁴ Employees at the State office share these master security ID and passwords and,
- another FSA county office required all its employees to provide their passwords to another employee who locks these passwords in a safe. For example, if someone tampers with the application using employee A's password, but employee B also has access or knows the password, it will be difficult to establish which employee damaged the system.
- The password change interval is set at 90 days on the operating system. Cyber Security (CS) requires passwords for all systems, applications or processes to be changed every 60 days

¹ Logical access is the ability that users have to use, change, or view a computer system. To control that access means to restrict their ability to interact with the system. Logical access controls can be built into the operating system (e.g., automatically logging a user out after a period of inactivity), or incorporated into the applications that run on that system (e.g., passwords) (NIST 800-12 ch. 17).

² NIST 800-14, "Generally Accepted Principles for Securing IT Systems," Sept. 1996, sect. 3.11.3.

³ FSA Handbook 2-IRM, "Computer Operations for the GSS A and B," May 29, 2003, para. 281.F(5).

⁴ MO Notice IRM-36, "ADP Password Changes," December 8, 2003, Exhibit 3.

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.⁵ By leaving the passwords the same for longer than recommended, the agency increases the risk that an unauthorized user will gain and retain access to the application.

- In two county offices we visited, the computers did not automatically logout the user after a period of inactivity. Leaving open conduits into the application makes the application vulnerable to tampering and enhances the risk of exposing sensitive information to unauthorized access.

Combined, these logical access control weaknesses increase FSA's price support loan application vulnerability to misuse. Should an unauthorized user exploit these weaknesses, FSA's ability to establish accountability will be hampered since employees will have access to other employees' passwords.

Recommendation 3

Revise FSA direction on logical access control guidance to be consistent with Departmental requirements. Revise agency, State, and county directives to instruct FSA employees on new password requirements implemented and to properly safeguard master security IDs and passwords.

FSA Response.

In its August 1, 2005, response, FSA agreed with the recommendation. Also, FSA Handbook 2-IRM will be revised to direct users to change their passwords every 60 days and to not include passwords when preparing a list of User IDs. A notice will be issued directing State and County personnel to update all local directives to comply with these changes. Also, ITSD plans to implement these corrective actions before October 1, 2005.

OIG Position.

We accept management decision for Recommendation 3. For final action, FSA will need to report to the OCFO that the proposed actions have been accomplished.

⁵ CS-13, "Passwords," Chapter 6 Part 5, "Controlled Access Protection (C2)", March 6, 2002, sect 2.

Recommendation 4

Ensure that employees who have made their passwords and IDs available to others obtain new unique passwords and user IDs. Set computer system password and workstation logout controls, as required, by Departmental security guidance.

FSA Response.

In its August 1, 2005, response, FSA indicated that user passwords will be changed according to the 60 day cycle. Any employees who have made their passwords and ID's available to others will be instructed to reset their passwords and not share their ID's or passwords with others. Every employee will have a unique ID with a password known only to the employee. It is not feasible to issue new user ID's. The User IDs have been stored in numerous audit trail files. The new User ID would start out as a completely new user with no way to link the new User ID to the activities of the old User ID.

The IBM S/36 does not have an option to logout a user after a specified time. If a disconnection is forced from a higher level (network or AS/400 hosting system), the hard termination of a users session can cause data corruption in many of our applications. The S/36 does not have a database management system with commit/rollback capabilities. If a user is in the middle of a transaction and their session gets terminated, half of a transaction may be recorded. Implementing a forced disconnection would present a larger risk than the one we would be trying to mitigate. Also, ITSD will instruct employees to change their passwords by the end of the Fiscal Year (or sooner).

OIG Position.

We accept management decision for Recommendation 4. For final action, FSA will need to report to the OCFO that the proposed actions have been accomplished.

Finding 3

Remote Access Security Needs Strengthening

FSA does not have adequate control over external access to information contained within its price support loan application. FSA management did not institute security controls that were capable of encrypting⁶ data in some locations because they believed the cost was too high, and the

⁶ Encryption is the process of disguising information or data so that it is unintelligible to an unauthorized person.

encryption, or other security transmission measures, significantly slow the transmission through the transmission method used to an unacceptable level. This decision left the data at risk of being compromised.

We found that about 155 of 2,500 FSA service centers do not encrypt information before transmitting it to FSA's main computer system. The 155 service centers transmitted sensitive information, including information on about 2,600 loans, totaling \$163 million made for crop year 2002 using an inappropriate method. Without encryption or other security transmission measures, sensitive information is not adequately protected. USDA standards⁷ state that all USDA ADP installations should protect sensitive data by use of file level passwords, read/write locks, and/or encryption. These same standards⁸ advocate that all USDA ADP installations consider encrypting sensitive data to protect it while being transmitted via telecommunications. In addition, DM 3550-002⁹ now clarifies that sensitive, but unclassified information, transmitted by frame relay, is to be encrypted.

FSA has neither required that the county offices submit their data securely, nor replaced the transmission method to allow encryption to be utilized for these 155 locations. Agency officials indicated that they believed the cost to switch to a transmission method that enables encryption to be acceptably used was prohibitive, based on the small activity level in these locations.

Recommendation 5

Consult with the Office of the Chief Information Officer (OCIO) and implement adequate security to ensure that all sensitive data is transmitted securely, in accordance with Departmental and federal encryption requirements and update agency procedures, as needed.

FSA Response.

In its August 1, 2005, response, FSA indicated that the majority of FSA service centers encrypt data before transmission to FSA's central computer systems. Approximately 155 service centers are currently unable to use Virtual Private Network conduits to transmit their data with encryption. These are small, low volume service centers. Given the current budget constraints and possible future office consolidations, as well as current efforts to migrate existing *AS/400* applications to a central web environment, it is not cost effective to dedicate resources to

⁷ DM 3140-1, Management ADP Security Manual, section 15 (b).

⁸ DM 3140-1, Management ADP Security Manual, section 18.

⁹ DM 3550-002, Sensitive but Unclassified Protection Information, chapter 10, part 2, table 3 dated February 17, 2005.

implement this type of security for 155 low volume sites. FSA is consulting with OCIO's Information Technology Services (ITS) on this issue. ITS, which is now responsible for FSA's Information Technology (IT) infrastructure, is looking into this issue and may request a waiver to Departmental requirements in this area. Also, the FSA response indicated that OCIO plans to submit a waiver request by August 15, 2005.

OIG Position.

Management decision for Recommendation 5 is contingent on the pending OCIO decision regarding the waiver of Departmental requirements. If a waiver is not granted, a corrective action plan that shows how the 155 sites will transmit data in accordance with Departmental regulations and applicable timeframes is needed. For final action, FSA will need to report to the OCFO that the proposed actions have been accomplished.

Section 3. Documentation

Finding 4

Inadequate Risk Assessment Documentation

The documentation used by a contractor FSA hired to perform a risk assessment for its price support loan application did not include all relevant information to provide an accurate assessment. The contractor did not include a network topology—essentially, a blueprint of the computer network—that should have been reviewed prior to determining the risks associated with the application, as well as omitting other crucial information. FSA believed that the contractor had this knowledge, but it did not pursue obtaining the documentation from the contractor. As a result, FSA could not be assured that the risks attributable to its mission-critical system have been considered and that appropriate steps have been taken to mitigate these risks.

NIST guidance for a risk assessment of an IT system requires an understanding of the system's processing environment. To perform a risk assessment, some system-related information must be collected. A current network topology is one of the additional documents needed to develop a knowledge of the environment and operations of the IT system and its data.

We reviewed the assessment completed in May 2003, by FSA's contractor. The assessment lacked (1) a network topology, (2) a list of APSS personnel (of which, the price support loan application is a part), and (3) information about a database used to update information about loans and loan deficiency payments made to producers. Instead, there were blank highlighted sections that an FSA official indicated were for FSA staff to insert specific names or information at some later date.

FSA's risk assessments were in the process of being updated and completed in support of the certification and accreditation requirements at the time of our review. The documentation showed that as of February 2004, no topology had been included in the assessment. In March 2004, two FSA officials said that there was no network topology available for FSA's APSS and, by connection, the price support loan application. In April 2004, FSA stated that one contractor had performed the risk assessments for all of FSA's computer systems and should be familiar with the network topology. The FSA has recently completed the certification and accreditation process and the topology is now included.

Recommendation 6

Conduct sufficient reviews of completed risk assessments, and ensure each risk assessment includes documentation establishing that all needed elements have been considered as part of the assessment's development (e.g., network topology, list of system personnel, and connected applications) prior to acceptance of the work and payment of the contractor.

FSA Response.

In its August 1, 2005, response, FSA indicated that as part of the Certification and Accreditation (C&A) process for the APSS (completed September 2004), the risk assessment (RA) document was updated to include all required elements. FSA follows current Department of Agriculture C&A guidelines in reviewing the RA, and FSA will work to ensure that all needed elements are contained in future RA documents. Also, FSA has indicated they are already in compliance with the recommendation; therefore, no further action is needed.

OIG Position.

We accept management decision for Recommendation 6. For final action, FSA will need to report to the OCFO that the corrective actions have been accomplished.

Finding 5

Contingency Plans Need Revision

FSA's contingency plans for county offices to continue operation of their price support loan application, in the event of disaster, does not reflect the expected recovery actions to be taken. Specifically, the alternate sites designated to carry on operations did not have the computing capacity to effect the application. In prior emergencies that shut down an office's application (e.g., tornadoes), FSA had sent personnel and equipment to restore operations rather than following the contingency plan procedures the agency put in place. These ad hoc recoveries, however, are not explained or formalized within the county offices' written plans.

NIST 800-12 calls for agencies to plan how to keep their critical functions operating in the event of disruptions as an essential element

of contingency planning.¹⁰ As the final step in planning, an agency must test the plan along several dimensions to make sure that it will work to continue operations.¹¹

We reviewed the plans for three county offices to determine if they were sufficient to restore operations in the event of a disruption. Each of the offices had agreements with their neighboring county offices to run the application on their computers in cases of system failure. In all three cases, the offices' computers, however, did not appear to have enough disk space to upload the neighboring office's systems and continue to run their own workload as well.¹² According to disk space capacity reports, each office was using 57 percent of its own disk space for part of its operating system. Consequently, running the systems of two offices together might exceed the disk space available.

In one State office, FSA officials acknowledged that some parts of the contingency plans could be improved. In two other State offices, they stated that they relied on agency personnel to restore their system with new equipment and programs. These personnel informed us that they had prepared their plans using the guidance provided in FSA procedures. FSA headquarters personnel stated that they usually provide the required equipment to the disabled county.

Relying on FSA headquarters personnel does not supplant the need for a formal contingency plan that outlines the actual steps that a county office must take to recover operations.

Recommendation 7

Revise contingency plans for all county offices that will provide for achievable processes to be followed for continued operation of the application, if an emergency arises. Establish oversight of the plans to ensure that they accurately describe expected actions.

FSA Response.

In its August 1, 2005, response, FSA indicated that Finding 5 (Contingency Plans Need Revision) appears to focus on the need for additional documentation covering all of the various options available to recover county office operations in the event of an emergency, service disruption, or hardware failure. While the FSA contingency plan for county offices does reflect the expected recovery actions to be

¹⁰ Chapter 11.

¹¹ Chapter 11.6.

¹² The AS/400 System 36 is an integrated system where the AS/400 provides the platform and core operating system for the Advance System 36 emulation. System 36 is required for most state and county office legacy applications to operate.

taken, it is true that options, other than the transfer of operations to an alternate site, have been used in order to recover operations. These options may include replacing failed or damaged hardware, moving hardware from a disaster site to a suitable alternate location, or using existing hardware at an alternate site to continue operations. Step-by-step procedures covering each of these options, as well as criteria for selecting an appropriate recovery option, should be incorporated into an updated contingency plan.

FSA also disputed that the disk space capacity may not allow both offices running the applications for two service centers in that two copies of the operating system and application libraries are not required. Only the data files from the disaster site need to be loaded upon the system at the alternate site. Therefore, the actual amount of space required for establishing the disaster site on the alternate system will be significantly lower than the sum of the two disk space utilization figures. Also, FSA has indicated they are already in compliance with the recommendation; therefore, no further action is needed.

OIG Position.

We were unable to accept management decision for Recommendation 7 without additional clarification regarding whether FSA will or has issued step-by-step procedures covering each of the recovery options, the criteria for selecting an appropriate recovery option, and how this option should be incorporated into each county office updated contingency plan. Also, information is needed detailing the procedures to provide oversight of the plans to ensure that they accurately describe expected actions along with the timeframes.

Scope and Methodology

Our audit was part of a nationwide audit of selected USDA agencies and selected applications within these agencies. We tested an application contained within the APSS to determine if selected application system controls (manual or automated) are in place and functioning effectively to ensure transactions are properly authorized, completely processed, and accurately processed. The APSS consists of price support loans, price support loan deficiency payments, and price support graze out payments.

We selected FSA's price support loan application, based on the size of the application and the type of processing it conducted. We conducted our review through interviews, review of FSA procedures and records, and observations.

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

- Gained an understanding of the FSA IT environment;
- Reviewed agency, Departmental, and other Federally mandated IT security policies and procedures;
- Interviewed responsible officials for managing the price support loan application, and reviewed and analyzed FSA records;
- Performed detailed testing of FSA's logical and physical access controls for one mission-critical application, and software controls by analyzing records and controls established to ensure the security of FSA's price support loan application; and
- Conducted testing at Kansas City, Missouri, Beacon Facility and three county offices in three States.

Audit fieldwork was performed from February 2004 through August 2004. The audit was conducted in accordance with Government Auditing Standards.

Exhibit A – FSA Response

Exhibit A – Page 1 of 7



AUG 1 2005

United States
Department of
Agriculture

Farm and Foreign
Agricultural
Services


Farm Service
Agency

Operations Review
and Analysis Staff

Audits,
Investigations and
State and County
Review Branch

1400
Independence
Avenue, SW
Stop 0540
Washington, DC
20250-0540

TO: Director, Farm and Foreign Agriculture Division
Office of Inspector General

FROM: Philip Sharp, Chief 
Audits, Investigations, and State and County Review Branch

SUBJECT: Response to Request for Information: 03099-195-KC – Price Support
Loan Application

Attached are copies of memoranda from the Farm Service Agency's Director of the Price Support Division and the Acting Director of the Information Technology Services Division responding to your request for a response to the subject audit report.

Following are the target dates for completing the cited recommendations:

- Recommendation 2, the target date for completing final action is August 31.
- Recommendation 3, ITSD plans to revise handbook 2-IRM and issue a notice to update local directives this fiscal year (FY), i.e. before October 1, 2005, if management decision is reached on this item.
- Recommendation 4, employees would be instructed to change their passwords by the end of the FY (or sooner), if management decision is reached on this item.
- Recommendation 5, OCIO's Information Technology Services (ITS), which now manages FSA's (and RD's and NRCS's computer infrastructure) has informed me that they plan to submit a waiver request by August 15. Further developments will depend on if the Department approves ITS' waiver request.
- Recommendations 6 & 7, ITSD believes it is already in compliance with OIG's recommendations and no further action is needed.

Please address any questions to Karren Fava 720-6152.

USDA is an Equal Opportunity Employer



JUL 26 2005

United States Department of Agriculture

Farm and Foreign Agricultural Services

Farm Service Agency

1400 Independence Avenue, SW
Stop 0512
Washington, DC
20250-0512

TO: Philip Sharp, Chief
Audits, Investigations, State and County Review Branch

FROM: Grady Bilberry, Director
Price Support Division

SUBJECT: OIG Audit Report 03099-195-KC Price Support Loan Application

*Mc
FAS
7-26-05*

OIG Audit No. 03099-195-KC provided results of the price support loan application within the Automated Price Support System (APSS) and your office requested responses to Findings 1 through 5. PSD will respond to Finding 1 of this Audit and responses to Findings 2 through 5 will be provided by ITSD under a separate memorandum.

Finding 1

FSA lacks assurance that the price support loan application is correctly programmed to validate data.

Recommendation 1

Conduct a detailed analysis of the adequacy of the key validation controls for the price support application.

Recommendation 2

Develop and document validation controls to mitigate the specific weaknesses cited above and those identified during the detailed analysis.

FSA Response

We agree with Recommendations 1 and 2 and PSD conducted a preliminary detailed review and analysis specific to the weaknesses addressed in Finding 1. The five validation weaknesses cited in your audit pertaining to the marketing assistance loan applications were as follows:

- accepted crop loans 2 months after the final loan availability date
- permitted users to change interest rate tables, established yield tables, and service fees
- prevented users from entering accurate information relating to test weight
- allowed for input changes, such as quantity and alpha responses

USDA is an Equal Opportunity Employer

- allowed inaccurate State codes to be entered.

Of the weaknesses cited, we developed a validation control to accept a marketing assistance loan application within the final loan availability period applicable to the corp. This software enhancement will be released in County Release 568 and is scheduled to be released on July 25, 2005.

Our analysis found one screen where the alpha other than "Y" or "N" was permitted to a question requiring a yes or no response. We will issue a user requirement to request an enhancement to this validation. The user requirement will be completed by August 31, 2005.

We also found through our analysis that APSS does validate against test weight that is not applicable to a specific commodity. For example, a test weight of 50 is not applicable to the standards for corn and APSS prohibited this entry. However, a test weight of 50 is applicable to barley and therefore was accepted through APSS.

Human interaction is required for the remaining weaknesses cited in the audit which make an automated validation impossible. However, we will issue a directive to the State and county offices reminding them of the procedure for maintaining table files and to ensure program validations are correctly applied.

We are in the beginning stages to develop a web based eLOAN application process via the internet. When this is completed, the APSS will not be needed to support marketing assistance loans. The user requirement was issued to address this project on June 26, 2005. A more in-depth validation system will be implemented with this process in all activities pertaining to all programs currently used by APSS.

Because all resources are assigned to the eGOV initiatives, any additional enhancements to APSS may be prohibited as directed by our Administration and ITSD. However, we will make every attempt to ensure that validations remain a top priority in development of software.



JUL 26 2005

United States
Department of
Agriculture

Farm and Foreign
Agricultural
Service

Farm Service
Agency

1400 Independence
Ave, SW
Stop 0580
Washington, DC
20250-0580

TO: Phillip Sharp
Chief
Audits, Investigations and State and County Review Branch

FROM: Steven L. Sanders
Acting Director
Information Technology Services Division

ATTENTION: 03099-195-KC

SUBJECT: Comments on Information Technology (IT) Audit Findings in the Discussion Draft Audit Report for the Farm Service Agency (FSA) Price Support Loan Application, Report No. 03099-195-KC

Handwritten notes:
3m
FAS
7-26-05
Hudson for Steve Sanders

Background

The Director of FSA's Price Support Division (PSD) has the lead in coordinating the official response with the Information Technology Services Division (ITSD). The Deputy Director of PSD, Ms. Raellen Erickson, requested that ITSD respond directly to Audits, Investigations and Stated and County Review Branch on the IT related findings and recommendations and provide PSD with a copy. ITSD is providing this response as requested.

OIG Finding 2—Logical Access Controls Security Need Strengthening

OIG Recommendation No. 3

Revise FSA direction on logical access control guidance to be consistent with Departmental requirements. Revise agency, State, and county directives to instruct FSA employees on new password requirements implemented and to properly safeguard master security identifications (IDs) and passwords.

FSA Response:

FSA agrees with Office of the Inspector General's recommendation. FSA Handbook 2-IRM will be revised to direct users to change their passwords every 60 days and to not include passwords when preparing a list of User IDs. A notice will be issued directing State and County personnel to update all local directives to comply with these changes.

USDA is an Equal Opportunity Employer

OIG Recommendation 4

Ensure that employees who have made their passwords and ID's available to others obtain new unique passwords and user ID's. Set computer system password and workstation logout controls as required by Departmental security guidance.

FSA Response:

User passwords will be changed according to the 60 day cycle. Any employees who have made their passwords and ID's others will be instructed to reset their passwords and not share their ID's or passwords with others. Every employee will have a unique ID with a password known only to the employee. It is not feasible to issue new User ID's. The User IDs have been stored in numerous audit trail files. The new User ID would start out as a completely new user with no way to link the new User ID to the activities of the old User ID.

The IBM S/36 does not have an option to logout a user after a specified time. If a disconnection is forced from a higher level (network or AS/400 hosting system), the hard termination of a user's session can cause data corruption in many of our applications. The S/36 does not have a database management system with commit/rollback capabilities. If a user is in the middle of a transaction and their session gets terminated, half of a transaction may be recorded. Implementing a forced disconnect would present a larger risk than the one we would be trying to mitigate.

OIG Finding 3—Remote Access Security Needs Strengthening

OIG Recommendation 5

Consult with the Office of the Chief Information Officer and implement adequate security to ensure that all sensitive data is transmitted securely, in accordance with Departmental and federal encryption requirements and update agency procedures as needed.

FSA Response:

The majority of FSA service centers encrypt data before transmission to FSA's central computer systems. Approximately 155 service centers are currently unable to use Virtual Private Network conduits to transmit their data with encryption. These are small, low volume service centers. Given the current budget constraints and possible future office consolidations, as well as current efforts to migrate existing AS/400 applications to a central web environment, it is not cost effective to dedicate resources to implement this type of security for 155 low volume sites.

Philip Sharp

Page 3

FSA is consulting with OCIO's Information Technology Services (ITS) on this issue. ITS, which is now responsible for FSA's IT infrastructure, is looking into this issue and may request a waiver to Departmental requirements in this area.

OIG Finding 4—Inadequate Risk Assessment (RA) Documentation

OIG Recommendation No. 6

Conduct sufficient reviews of completed RAs and ensure each risk assessment includes documentation establishing that all needed elements have been considered as part of the assessment's development (e.g. network topology, list of system personnel, and connected applications) prior to acceptance of the work and payment of the contractor.

FSA Response:

As part of the Certification and Accreditation (C&A) process for the Automated Price Support System (completed September 2004) the RA document was updated to include all required elements. FSA follows current Department of Agriculture C&A guidelines in reviewing RA and FSA will work to ensure that all needed elements are contained in future RA documents.

OIG Finding 5—Contingency Plans Need Revision

OIG Recommendation No. 7

Revise contingency plans for all county offices that will provide for achievable processes to be followed for continued operation of the application if and emergency arises. Establish oversight of the plans to ensure that they accurately describe expected actions.

FSA Response:

Finding 5 (Contingency Plans Need Revision) appears to focus on the need for additional documentation covering all of the various options available to recover county office operations in the event of an emergency, service disruption, or hardware failure. While the FSA contingency plan for county offices does reflect the expected recovery actions to be taken, it is true that options other than the transfer of operations to an alternate site have been used in order to recover operations. These options may include replacing failed or damaged hardware, moving hardware from a disaster site to a suitable alternate location, or using existing hardware at an alternate site to continue operations. Step-by-step procedures covering each of these options, as well as criteria for selecting an appropriate recovery option should be incorporated into an updated contingency plan.

Philip Sharp
Page 4

The comment in Finding 5 that “According to disk space capacity reports each office was using 57 percent of its own disk space for part of its operating system. Consequently, running the systems of both offices together would exceed the disk space available to either office by about 14 percent” is inaccurate. The alternate sites already have the application libraries as well as the operating system needed to run applications for both service centers. Two copies of the operating system and application libraries are not required. Only the data files from the disaster site need to be loaded upon the system at the alternate site. Therefore, the actual amount of space required for establishing the disaster site on the alternate system will be significantly lower than the sum of the two disk space utilization figures.

For More Information

If you have questions or need any more information, please contact me at 202-720-7796, or contact Brian J. Davies, Acting Chief, Information Security Office, at 202-720-2419.

Informational copies of this report have been distributed to:

Administrator, FSA	
ATTN: Agency Liaison Officer	(6)
Government Accountability Office	(1)
Office of Management and Budget	(1)
Office of the Chief Financial Officer	
Director, Planning and Accountability Division	(1)