



U.S. Department of Agriculture
Office of Inspector General
Great Plains Region
Audit Report

Farm Service Agency/
Commodity Credit Corporation
Security Over Information Technology
Resources



Report No.
03099-47-KC
October 2001



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL



Washington D.C. 20250

DATE: October 31, 2001

REPLY TO
ATTN OF: 03099-47-KC

SUBJECT: Farm Service Agency/Commodity Credit Corporation - Security Over
Information Technology Resources

TO: James R. Little
Administrator
Farm Service Agency

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

This report represents the results of the subject audit. The written response, dated September 28, 2001, has been incorporated into the Findings and Recommendations section of the report. The text of the response is attached as exhibit A. The response and our comments are presented in the Findings and Recommendations section of the report and explain actions and/or information necessary to achieve management decisions on Recommendations Nos. 2, 4, 5, 6, 7, 9, 10, 11, and 12. We have accepted the management decision for Recommendations Nos. 1, 3, and 8.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing corrective actions taken or planned and the date when final action is anticipated. Please note that the regulation requires management decisions to be reached on all findings and recommendations within 6 months from the date of report issuance. Follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer for those recommendations where management decision has been reached.

We appreciate the assistance you and your staff provided to us during our review.

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

FARM SERVICE AGENCY/ COMMODITY CREDIT CORPORATION SECURITY OVER INFORMATION TECHNOLOGY RESOURCES

REPORT NO. 03099-47-KC

RESULTS IN BRIEF

The main objectives of our audit were to (1) assess the threat of penetration of Farm Service Agency (FSA)/Commodity Credit Corporation (CCC) payment and/or data systems, (2) determine the adequacy of the security over the Local and Wide Area Networks (LAN/WAN), and (3) assess FSA/CCC management's involvement in Information Technology (IT) security.

Based upon our reviews at Washington, D.C., Kansas City, Missouri, and five other field sites, we concluded that FSA management needed to increase their involvement in computer security to minimize the threat of penetration of payment and data systems. We found that an FSA computer had been used to access prohibited Internet websites. Further research disclosed that the user had been the supervisor of a wiring contractor team that had been left unattended in the office after regular working hours. At another site, the systems administrator/security officer acknowledged it was common practice to share logon identification numbers (ID's) with visitors rather than create restricted access guest ID's. At this same site, we found an extra systems administrator (unlimited access) logon that was known to the security officer but could not be explained. We found that some sites relied primarily on a single individual for systems administration and security. These sites were more susceptible to service disruption if something were to happen to these employees.

We also found physical security weaknesses at most sites. Computer servers and related supplies were not always located behind lockable doors. However, when they were, the doors remained unlocked and most personnel had access. Even in a facility considered by the Agency to be secure, we noted weaknesses. At this facility, our review of access logs disclosed that 112 personnel, outside of the responsible Division, had physical access to the server room. Further research disclosed that a Division separate from the operational Division controlled access authority.

We found that some of the more sophisticated tools for protecting computer networks were not fully utilized. Our scans of 121 network components disclosed a total of 252 high and medium-risk vulnerabilities that could make FSA systems subject to attack. They ranged from failure to change default settings to a large number of unused logons whose associated passwords were set to never expire. The scan results were shared with FSA officials as the scans were completed. Where feasible, FSA officials took immediate corrective actions.

Simple tools such as workstation locking were not always used and controls were not adequate to ensure that user accounts were deleted when personnel left FSA. Additionally, we noted that FSA had not taken adequate actions to ensure that employees were not using Government computer resources to visit prohibited Internet websites.

System security plans were not always used as a tool to help improve security. Associated risk assessments were not completed at the required intervals and security plans did not provide a management structure indicating system responsibilities. In addition, contingency planning was treated more as an annual requirement than an opportunity to test emergency planning for service continuity. We also found that plans were not always updated to reflect significant changes, nor were they tested on an annual basis.

KEY RECOMMENDATIONS

We recommended that FSA take immediate action to eliminate the high and medium vulnerabilities identified by the scans, implement a policy of regular scans with corrective action, and remove all unnecessary accounts from networks. We further recommended that FSA issue one or more Information Resource Management (IRM) Notices that reminded personnel of their responsibilities to protect sensitive program data and require system administrators to perform an immediate reconciliation of logon ID's and system users to identify and delete any obsolete ID's. We also recommended that FSA review and strengthen their physical security, where feasible. Additionally, we recommended that FSA implement a procedure allowing the security staff to immediately report inappropriate systems usage to responsible managers. We also recommended that, in conjunction with the implementation of computer system upgrades, FSA develop a set of guidelines that will provide for additional oversight in those locations where a lack of resources limits the potential for segregation of duties.

AGENCY RESPONSE

In its response dated, September 28, 2001 (see exhibit A), FSA concurred with the Findings and Recommendations and stated that actions had been taken or were being planned to address each of the weaknesses cited in the report.

OIG POSITION

We concur with the actions taken or proposed by FSA on the recommendations and have reached management decision on Recommendation Nos. 1, 3, and 8. In order to reach management decision for the remaining recommendations, we will need to be provided timeframes for accomplishing the agreed upon actions.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
RESULTS IN BRIEF	i
KEY RECOMMENDATIONS	ii
AGENCY RESPONSE	iii
OIG POSITION	iii
TABLE OF CONTENTS.....	iv
INTRODUCTION.....	1
BACKGROUND	1
OBJECTIVES.....	2
SCOPE	2
METHODOLOGY	2
FINDINGS AND RECOMMENDATIONS	4
CHAPTER 1	4
ACCESS CONTROLS NEED IMPROVEMENT	4
FINDING NO. 1	5
RECOMMENDATION NO. 1	7
RECOMMENDATION NO. 2	7
RECOMMENDATION NO. 3	7
FINDING NO. 2	8
RECOMMENDATION NO. 4	10
FINDING NO. 3	11
RECOMMENDATION NO. 5	12
FINDING NO. 4	12
RECOMMENDATION NO. 6	13
CHAPTER 2	15
GENERAL CONTROLS COULD BE MORE EFFECTIVE	15
FINDING NO. 5	15

RECOMMENDATION NO. 7	16
FINDING NO. 6	16
RECOMMENDATION NO. 8	17
CHAPTER 3	18
INADEQUATE SEGREGATION OF DUTIES NOT COMPENSATED FOR BY SUPERVISORY REVIEW.....	18
FINDING NO. 7	18
RECOMMENDATION NO. 9	19
CHAPTER 4	20
DISASTER RECOVERY PLANS WERE NOT CURRENT.....	20
FINDING NO. 8	20
RECOMMENDATION NO. 10	21
RECOMMENDATION NO. 11	21
RECOMMENDATION NO. 12	22
GENERAL COMMENTS.....	23
EXHIBIT A – AUDITEE RESPONSE TO DRAFT REPORT.....	24
ABBREVIATIONS.....	33

INTRODUCTION

BACKGROUND

The 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 FSA and the State and county committees. There are 50 FSA State offices and about 2,150 county offices. Additionally, the FSA maintains field office personnel in Kansas City and St. Louis, Missouri, and Salt Lake City, Utah. FSA personnel total about 15,000. Utilizing these personnel, FSA and CCC expended funds totaling over \$29 billion for fiscal year (FY) 2000.

Expenses for the acquisition, operation, maintenance, improvement, or disposition of property, including IT resources which the CCC owns, have been treated as program expenses. Beginning in FY 1992, the FSA started receiving a direct appropriation for these types of operating expenses. Section 161 of the Federal Agriculture Improvement and Reform Act of 1996 placed limits upon the amount of CCC funds that could be used for operating expenses. Therefore, the FSA has been limited in the amount of directly appropriated or CCC program funds that might be spent for the acquisition of IT resources.

Since 1985, all State and county FSA offices have used automated systems to support their day-to-day program operations. Replacements of the FSA legacy systems are now being accomplished under the United States Department of Agriculture Service Center Initiative. Phase 1 of the Service Center Shared Information System was initiated in 1998 and included the purchase of desktop and laptop computers to replace computers that were not Y2K compliant and to implement and initiate Common Computing Environment capability. Another phase of the Service Center Initiative is the LAN/WAN/VOICE project begun in FY 1996. This project will result in integrated telephone systems; LAN/WAN needed for sharing data, technology, and information; an integrated E-mail system; and optimization of phone and data circuits to support the

combined traffic load at least cost. Various laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995. 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 ADP Security Manual, and various Departmental Regulations (DR).¹ Additionally, the FSA has issued certain security guidelines in a series of IRM Handbooks².

OBJECTIVES

The audit objectives were to (1) assess the threat of penetration of FSA/CCC payment and/or data systems, (2) determine the adequacy of the security over the LAN/WAN, and (3) assess FSA/CCC management's involvement in IT security.

SCOPE

To assess FSA's IT security, we tested computer systems in the Washington D.C. headquarters, in Kansas City, Missouri, and five field sites. The field sites were selected to represent a broad spectrum of FSA operations; including support sites that did not disburse payments directly to producers, one site that maintained a county level website, and one site that was part of the Business Process Reengineering/Common Computing Environment pilot test. This test site represents the type of operation that FSA is moving towards. Field visits were made between August and December 2000.

The audit was conducted in accordance with Government Auditing Standards.

METHODOLOGY

To accomplish our audit objectives, we interviewed responsible security officials at each site to determine their security procedures and evaluated the security structure to determine if it maintained an adequate segregation of duties

¹ DR 3130- 2, Microcomputer Policy, 3140-1, USDA Information Systems Security Policy, 3140-2, USDA Internet Security Policy, and 3300-1, Telecommunications & Internet Services and Use.

² 2-IRM, Computer Operations, 4-IRM, FTS Mail Management, 5-IRM, Telecommunications Management, and 6-IRM, Guidelines for Developing ADP Security Plans in SCOAP Facilities.

over incompatible tasks. Additionally, scans were performed of 121 selected network components to assess their vulnerability to attack. At each field site, we observed physical security to determine if hardware and computer supplies were protected from theft, destruction, or compromise. We tested logical security to determine if system access was limited to authorized users. Password rules were reviewed and compared to best practice policies. We checked computer files to determine if users had been accessing prohibited websites. Backup tape logs were reviewed where available. Security plans, risk assessments, and contingency plans were reviewed to determine if they were adequate and up-to-date. We also evaluated the procedures in place to prevent and/or detect unauthorized intrusions.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	ACCESS CONTROLS NEED IMPROVEMENT
------------------	---

Our reviews disclosed that FSA did not have controls adequate to ensure that LAN/WAN access was limited to authorized individuals and/or for authorized purposes. We also found weaknesses in logical security that would render FSA systems more vulnerable to penetration. We found weaknesses in physical security that rendered FSA IT resources more vulnerable to loss, theft, or misuse. The belief by local management that the current technology was secure has helped create an environment where IT security receives a low priority.

Access controls should provide reasonable assurance that computer resources (data files, application programs, computer related facilities, and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Access controls are composed of logical and physical controls. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user ID's, passwords, or other identifiers that are linked to predetermined access privileges. When telecommunications are involved, specialized software and hardware is available to limit access by outside systems or individuals. These include firewalls, teleprocessing monitors, communications port protection devices, and smart cards. Logical controls should be designed to restrict legitimate users to the specific systems, programs, and files that they need, and prevent others from accessing any computer resources. Additionally, logical controls should be used to produce and analyze audit trails of system and user activity and take defensive measures against intrusion. Physical access control involves restricting access to computer resources, usually by limiting access to the buildings and rooms where the resources are housed, or by installing physical locks on workstations. Physical controls also pertain to the storage and withdrawal of tapes or other storage media to and from the library or offsite storage.

FINDING NO. 1
NETWORK SECURITY
ASSESSMENTS REVEALED
VULNERABILITIES

Our scans of FSA computer networks disclosed numerous weaknesses. As a result, FSA computer networks were more vulnerable to outside attack. FSA personnel agreed with these findings and are actively working to correct the problems noted.

As part of our audit, we scanned 121 computer network components at the FSA Headquarters in Washington, D.C., in Kansas City, Missouri, and two field sites. For these assessments, we utilized an off-the-shelf software product which is designed to identify vulnerabilities associated with various information technology platforms. The software performs over 800 tests for security vulnerabilities that use Transmission Control Protocol/Internet Protocol (TCP/IP).

The scan reports disclosed a total of 1,216 vulnerabilities: 40 high-risk, 212 medium-risk, and 964 low-risk. High-risk vulnerabilities are those that provide access to the computer and, possibly, the computer network. Medium-risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low-risk vulnerabilities are those that provide access to network data that might be sensitive but is less likely to lead to a higher risk exploit.

High-risk vulnerabilities included: (a) a weakness in a program used to send electronic mail that could be used to execute commands on the system; (b) a protocol used to manage network hardware was configured with default settings, and (c) one file transfer protocol that could prevent legitimate users from accessing files and another that could allow an attacker to execute programs as the systems administrator. At one location we found a high-risk vulnerability that would allow anyone the ability to change the host's system information. We found one vulnerability that was rated as low-risk but is included due to the large volume of occurrence on one system. This system contained 583 accounts that had never logged onto the system; 167 of which had passwords that were set to never expire.

We also conducted a detailed assessment of the security of the Novell network at Kansas City, Missouri. Our assessment software allowed us to compare FSA's established security practices to the actual settings on the Novell systems. We also compared the system's security settings to the software product's "best-practices settings," which are based on standard practices from a wide variety of government and private institutions. The software product reports weaknesses that may leave the system open to potential threats in the following areas: (1) account restrictions,

(2) password strength, (3) access control, (4) system monitoring, (5) data integrity, and (6) data confidentiality.

Our assessments disclosed significant weaknesses in account restrictions and access controls (the areas that define a user's ability to access the system). Some weaknesses we found included:

- 80 percent of containers (groups of network resources, such as users, printers, and/or servers that are divided along organizational or technical lines) do not have intruder detection turned on. The NetWare Intruder Detection feature limits the number of failed logon attempts a user can make. After a predefined number of failed logon attempts, NetWare assumes the user is an unauthorized intruder, adds an audit record to the system error log, and disables the account.
- 271 user accounts are hidden from the system administrator. This raises concern because hidden accounts are often used as a means to set up a "back door" to the server. These accounts hold administrator access privileges, privileges for most trusted users on a Novell system, which allow complete control of the system. Additionally, because of these privileges, unauthorized users can modify system logs to hide their activities from the system administrator.
- 22 percent of user accounts are inactive. User accounts that become inactive, but not disabled, provide opportunities for unauthorized users to gain access to the network. An attacker can try different passwords on these inactive accounts and attempt to gain access to the network. Once that access is gained, unauthorized activity cannot be traced to the responsible person.

The detailed results were shared with the responsible FSA personnel upon completion of the scans and they corrected all of the high and medium-risk vulnerabilities. The summary results of the TCP/IP scans were provided to FSA in Management Alert Nos. 03099-47-KC (1)³ and 03099-47-KC (2)⁴. FSA responded positively to the Management Alerts and has almost completed the recommended corrective actions.

OMB Circular A-130, Appendix III, states that agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

³ November 22, 2000

⁴ January 05, 2001

RECOMMENDATION NO. 1

Take immediate action to eliminate the high and medium vulnerabilities identified by the scan reports.

FSA Response

FSA stated that they concurred with the recommendation, and had completed corrective action on all of the high and medium-risk vulnerabilities, as well as the majority of the low-risk vulnerabilities.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 2

Implement a policy to perform scans on a regular basis and mitigate all weaknesses. Implement a policy of minimum security setting guidelines for Novell systems. Periodically assess the guidelines and determine if they remain appropriate.

FSA Response

FSA stated that they concurred with the recommendation and, effective March 1, 2001, had initiated a security policy to perform scans every 3 months and would scan monthly per a new Departmental policy. Follow-up scans are initiated once the weaknesses have been corrected. In addition, new servers are scanned as they are brought online to identify potential weaknesses.

OIG Position

We concur with proposed actions, but are unable to achieve management decision for this recommendation until we are informed whether FSA intends to periodically assess the guidelines and determine if they are still appropriate.

RECOMMENDATION NO. 3

Immediately remove unnecessary accounts from the networks and implement a system of controls that prevents the creation and retention of unnecessary accounts.

FSA Response

FSA stated that they concurred with the recommendation and the FSA security staff has reviewed the agency's clearance process for departing employees to ensure it is completed in a timely manner. LAN administrators are responsible for automatically suspending user identification codes that have been inactive for 30 calendar days. Additionally, FSA developed additional procedures, Inactive User Procedures, as a backup to assure unauthorized users are deleted from the networks. Reviews are made for inactive Novell users and used user accounts are disabled and later removed if they remain unused.

OIG Position

We concur with the management decision.

FINDING NO. 2

LOGICAL CONTROLS DID NOT ENSURE RESTRICTED SYSTEM USAGE

Our review disclosed that FSA personnel were not always making effective use of logical controls. The personnel tasked with systems administration generally did not understand that serious problems regarding logical access controls could evolve from inadequately monitored systems usage. As a result, FSA

managers cannot be sure that systems usage is restricted to legitimate users and authorized purposes and system users are not reducing the effectiveness of more sophisticated security measures.

We also noted that, despite DR's⁵ and Departmental high-level assurance to the contrary, a majority of FSA employees had the ability to access inappropriate websites. During the initial phases of this audit, OIG was informed that the USDA firewall policy was to prohibit the entry of certain specific traffic (pornography and gambling sites). However, our work at the State and county offices disclosed that the firewall did not prevent the entry of either type of prohibited website traffic. FSA State and county offices account for the majority of their personnel.

For example, we found one location where an outside contractor employee had made unauthorized use of FSA computer resources after normal business hours. The contractor employee used the site's only computer with an older operating system to access the Internet and visited some sites deemed inappropriate by the Department. This usage went undetected by the security personnel until our audit step, designed to check Internet usage, revealed some questionable sites. With the

⁵ DR 3300-1, Part 3, Special Instructions, Appendix I, Part 5, Policy.

assistance of the onsite security personnel, we were able to determine the sites visited by the contractor. The personnel stated that the contractor was licensed and bonded and they thought it safe to leave them unattended. Although our work did not reveal any other improper usage by the contractor, we could not be completely sure of the full extent of the computer usage or what other systems the contractor might have attempted to access. We immediately referred the unauthorized usage to the Agency for resolution.

DR 3140-2 states that USDA sponsored Internet connections are to be used for official USDA business. USDA personnel and contractors must not download from the Internet any pornography and must not use the Internet for private or personal business. Although updated policy allows for limited personal use of Agency systems, personnel are still restricted from accessing certain websites including those that provide pornography.

We found another location where FSA personnel were sharing ID's and passwords between employees and guests (visiting FSA personnel). The systems administrator stated that when a guest came to the office, and needed system access, one of the employees would log on and allow the guest to work under the employee's ID. This policy lessens accountability and control. We also found three field locations where active logon ID's existed for inactive personnel or could not be identified with a legitimate system user. In one case, we found an ID for an employee that had been separated for over 1 year. In another location, we found an ID having systems administrator capabilities. The systems administrator, although aware of the existence of this ID, did not know the identity of the user and was unsure how this ID had been placed on the system. Additionally, we found that at least two locations allowed infinite logon attempts without disabling the workstation. At the Washington, D.C., and Kansas City locations, we found 20 active LAN ID's for separated employees.

We also found that at one State office, three active employees did not have access authorization forms on file. At the corresponding county office, we found access authorization forms for only two of ten current employees⁶. At the other State office, we found access authorization forms for less than half of the active employees. This State office had a policy of not requiring access authorization forms for employees that had AS/400 workstation access without access to FSA mainframe computers or the Internet. The corresponding county office did not have forms for any of the employees and the responsible official was unfamiliar with the form.

⁶ These personnel were previously employed by the former Farmers Home Administration.

DM 3140-1 states that all ADP users are responsible for protecting ADP assets and data from theft, fraud, misuse, loss, or unauthorized modification. Users are to protect telephone numbers, passwords, and all other system access keys against unauthorized disclosure. When granting access to others, owners should limit the type and duration of access to the minimum necessary. Appendix D provides significant detailed instructions on the use of ID's and passwords.

RECOMMENDATION NO. 4

Issue an IRM Notice to all FSA employees reminding them of their responsibilities to protect sensitive program data. The Notice should emphasize how the sharing of passwords and failure to protect sensitive data can have an adverse impact on USDA programs and personnel. The Notice should also require each systems administrator to review the list of current user ID's, reconcile this to active employees, and delete user ID's for any inactive employees. Additionally, the Notice should remind systems administrators of their ongoing responsibility to ensure that user ID's are deleted as soon as an employee is separated from service with FSA.

FSA Response

FSA stated that they concurred with the recommendation and are in the process of developing a security handbook for all FSA personnel by the second quarter of 2002. FSA believed these weaknesses were limited in scope to specific State and county offices since the majority of its field offices are fully aware of their security responsibilities and are reminded periodically as required by the department as well as through annual computer security awareness training. In the meantime, they will issue an IRM notice to address the weaknesses identified in the finding and address general security "best practices." FSA has developed a comprehensive security awareness training program and is reviewing a web-based interactive training program for FY 2002.

OIG Position

We concur with the proposed action, but are unable to achieve management decision for this recommendation until we have received the timeframe for completing the proposed security notice.

FINDING NO. 3
PHYSICAL CONTROLS DO NOT
EFFECTIVELY RESTRICT ACCESS
TO SERVERS

Our review disclosed that physical access to computer servers was generally not restricted to systems administrators and access to other computer resources, such as system documentation and backup media, was not always adequately controlled. The responsible personnel generally did not

believe that there was a problem with their server access. As a result, the computer servers and related materials were subject to an increased risk of theft, damage, or other disruption.

We found physical access control weaknesses with computer servers in Kansas City and each of the five field sites visited. In the Kansas City Telecommunications Division, our review of access logs identified 112 non-Divisional personnel having access to the server room. These personnel included contractors, security guards, and FSA personnel from other divisions. Two field sites maintained their servers in locked rooms. However, we noted that one location did not keep the door to the room locked. At another field site, one server was housed in a metal and Plexiglas tower located in a common area. However, on the day we made our review of physical security, the tower was unlocked. This was attributed to a contractor working in the area. Another server at this site was contained in a locked room. However, on the day we performed our review, contractors were working on rewiring the building alarm system and the locking doors to the server room were left open for most of the day. This second site poses an additional challenge to physical security, because of its open design within a shared facility, where non-Agency employees have the potential to access FSA workstations.

In two other locations, we noted that the servers were contained in private rooms. However, the doors to these rooms did not have locks and were left open most of the time. In the fifth location, the server was left on a table in an open area. It should be noted that at one time this facility had a separate computer room with security and climate controls. However, a wall was removed resulting in lessened security. Additionally, we found at least two sites where not all personnel were using available keyboard-locking features to secure workstations when they were away from their desks.

DM 3140-1 states that ADP equipment should be located out of highly visible, heavily trafficked areas. Where possible, ADP activities should be shielded from casual observation. The facilities should be locked when not in use and data should be stored in locked rooms or cabinets.

RECOMMENDATION NO. 5

Keep servers and related materials within secured environments and limit access to systems administrators and their alternates. If access is required by others, adequate

monitoring should be provided. Ensure that available keyboard-locking features are utilized.

FSA Response

FSA stated that they concurred with the recommendation and stated that its Washington and Kansas City Headquarters network and telecommunication offices are fully secured and access is restricted according to USDA policy. Recently, the Office of Chief Information Officer (OCIO), Cyber Security Office, performed an onsite physical security assessment in Kansas City and made additional recommendations that FSA will address as funding is made available. With the implementation of the Common Computing Environment project, servers and LAN/WAN/Voice hardware will be stored and locked in specified security rooms. Additionally, forced screen savers and timeouts for users are being implemented on the Common Computing Environment platform.

OIG Position

We concur with the proposed actions, but cannot reach management decisions until a timeframe for accomplishing these planned actions is provided.

FINDING NO. 4
**INTERNET ACCESS NOT
SUSPENDED DURING
DISCIPLINARY ACTIONS**

Our review disclosed one instance where FSA could have taken additional actions when dealing with improper use of IT resources. Current procedure allows an employee to retain Internet access while disciplinary actions are being processed. As a result, there is increased vulnerability to additional

improper usage.

During our review, we were informed by FSA management of one employee that had been disciplined for improper usage of IT resources. Through discussion with other employees, we concluded that others in the Division were aware of this employee's acts. Follow-up with the Kansas City security staff disclosed that this employee continued to make improper usage of IT resources, even after the previous disciplinary action.

We also learned that the security staff did not restrict this employee's Internet access after subsequent improper acts. They forwarded their reports to the FSA personnel staff for action. However, the employee continued the improper usage during this time, as evidenced by Internet usage reports.

RECOMMENDATION NO. 6

Institute a procedure that allows the security staff to immediately report inappropriate systems usage to the responsible managers.

FSA Response

FSA responded that it cannot implement this recommendation at this time. Only the FSA Kansas City and St. Louis offices have a proxy server in place that requires employees to sign-on to the Internet using a user ID and password so we can track and block access. This function is not available in Washington, DC, State offices, nor our field office Service Centers.

FSA also responded that they follow a personnel process for Kansas City employees that involves the offending employee's immediate supervisor, a Personnel Relations Specialist, and a Security Office staff member. Once it has been determined that the charges against an employee have been substantiated and proved, Human Resources has the ability to notify the Security Office to suspend the Internet access of the employee for a specific period of time, if warranted, along with harsher penalties including suspension and removal. FSA does not consider this an issue within the Kansas City Office.

Suspending employees' Internet access in the field and Washington offices is a more complex technical issue. Washington, the field office Service Centers, and State offices are not configured to control access to the Internet through a central proxy server where access could be centrally managed, and there are no plans at this time for the Common Computing Environment to move in that direction. All of the vulnerabilities in the OIG audit were directed to specific field office sites where access is not being monitored. To shut off Internet access would require removing the web browser connection from the workstation.

Access for field office Service Centers would have to be managed at the OCIO firewall for this type of solution to be implemented, which is not in our control. OCIO is aware of this problem and is looking at providing some type of access monitoring tools at the OCIO device stack in the next

FY. Therefore, FSA cannot comply with this recommendation at this time, but will continue to make sure that FSA employees are made aware this is an offense that will not be tolerated.

OIG Position

In order for us to achieve management decision for this recommendation, we need to know what alternative actions FSA intends to take to ensure improper use of IT resources are not repeated by identified employees.

Our audit disclosed that FSA management had not always ensured the timely completion of required system reviews. A lack of resources had caused the completion of certain reviews to slip. Additionally, some of the reviews that had been completed did not contain all required information. As a result, there was additional risk of system problems going undetected by responsible officials.

An entity-wide program for security planning and management is the foundation of an entity's security control structure. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. The Computer Security Act of 1987 required agencies to identify and protect systems containing "sensitive" information and called for security training. OMB Circular A-130 established a minimum set of controls including; assigning responsibilities for security, security planning, periodic review of security controls, and management authorization of systems to process information.

FINDING NO. 5
REQUIRED RISK ASSESSMENTS
WERE NOT PERFORMED

Our review of the security plans and associated risk assessments for seven sensitive systems disclosed that four risk assessments were outdated. This condition was attributed to a lack of personnel. As a result, there was an increased potential that risks associated with system changes would not be identified and evaluated.

Our review of four sensitive systems security plans in Kansas City disclosed that none of the four referred to risk assessment nor did they otherwise identify any risk categories or levels of risk. Our discussion with the appropriate officials disclosed that a risk assessment had been performed in the past but it was now more than 3 years old and considered to be obsolete.

DM 3140-1 states that each agency will submit a security plan or an annual update to an existing plan annually. A security assessment should be conducted annually at each ADP processing site. The associated risk

assessment must be completed at intervals of 3 years or when hardware or system software undergo significant modification.

RECOMMENDATION NO. 7

Complete the risk assessment as soon as possible and implement a system of controls to ensure that risk assessments are completed on a yearly basis or as system

changes demand.

FSA Response

FSA concurred with the recommendation, and stated that the Security Office has prioritized the sensitive system applications FSA supports and maintains and will perform risk assessments on the 12 major sensitive systems for FY 2001. FSA has procured a software risk assessment package (Cobra) to assist it in performing these risk assessments. Funding has been included in the FY 2002 and 2003 to address additional risk assessments for the remaining systems.

OIG Position

We concur with the FSA proposal and can achieve management decision when informed of the timeframe for completion of the risk assessments for the remaining systems.

FINDING NO. 6**SECURITY RESPONSIBILITIES NOT CLEARLY ESTABLISHED**

Our review of the security plans for seven sensitive systems disclosed that three of the plans did not document a clearly established security management structure. As a result, we concluded that there is additional risk of system problems going undetected.

Our review of the security plan for one assessment accounting system, maintained in FSA Headquarters, disclosed that security responsibilities had been assigned to end-users rather than a responsible security official. Security plans for a commodity procurement system, Electronic Bid Entry, and a communication system, Telecommunications Software, did not include a security management structure. Without a documented security management structure there is less assurance that Agency security policies and procedures are being implemented and maintained.

The OMB states that responsibility for each major application should be assigned to a management official knowledgeable in the nature of the

information and process supported by the application⁷. This official should assure that effective security is used in the application and should be contacted in case of a security incident.

RECOMMENDATION NO. 8

Issue an IRM Notice requiring the owners of all sensitive systems to ensure that the next update of their security plan includes a documented security management structure.

FSA Response

FSA stated that they disagreed with the recommendation, but agreed with the need. They further stated that the OCIO had requested a new structured format for the 2001 annual system security plans which addresses the security management structure. FSA completed 113 major support security plans following the new format and the remaining applications will be addressed in this new format for FY 2002. FSA will continue to review all plans annually to assure this information is included in the security plans. FSA will also address this in its security handbook.

OIG Position

We accept the management decision.

⁷ OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, Part A.3.b

CHAPTER 3**INADEQUATE SEGREGATION OF DUTIES NOT
COMPENSATED FOR BY SUPERVISORY REVIEW****FINDING NO. 7**

Our review disclosed that not all field locations had adequate separation of duties due to staffing restrictions. We further noted that supervisory review did not compensate for the lack of segregation of duties. As a result, FSA

is exposing itself to additional risk of error or wrongful acts.

We found two locations where, primarily, one individual performed the office automation duties and responsibilities. No other personnel at these sites were tasked with oversight of the office automation function. The lack of segregation of duties and lack of oversight increases the potential that error or wrongful acts will occur and go undetected. One FSA function with the potential for oversight was the County Office Review Program (CORP) which performs periodic reviews of FSA county operations and targets reviews of individual program areas.

We reviewed the CORP report of common findings for 1999⁸. Section 6 of the Report stated that, out of 66 reports issued, only one common IT related finding was reported. The form FSA-765, Backup Log, was not being updated each time a backup was created. We also reviewed the CORP Handbook, Exhibit 7 (ADP Operations) to determine the nature of the CORP review. Because FSA had been using the IBM System 36 for automation, the review items were geared toward the System 36 environment and emphasized documentation and systems backup. The review guide did not contain any items geared, specifically, towards personal computer, LAN, or Internet usage. Based upon our review of these documents, we concluded that there were not sufficient compensating controls to ensure adequate security over smaller operations.

DM 3140-1, Appendix 6, Small Systems Security, provides some guidelines for offices where segregation of duties is not always possible. These guidelines include cross training of employees, monitoring of telecommunications and the reporting of any anomalies to management.

⁸ FSA Notice COR-92, dated April 4, 2000.

Work responsibilities should be segregated so that one individual does not control all critical stages of a process. Dividing duties among two or more individuals or groups diminishes the likelihood that errors or wrongful acts will go undetected because the activities of one will serve as a check on the other. The extent to which duties are segregated depends on the size of the organization and the risk associated with its activities. A large organization will have more flexibility in separating key duties. Smaller organizations may rely more on supervisory review to control activities.

RECOMMENDATION NO. 9

In conjunction with the implementation of upgraded field level servicing capabilities, develop a set of guidelines for providing supervisory review in offices where there is limited ability for segregation of duties.

FSA Response

FSA concurred with the recommendation and stated that they would address these concerns in their co-located Service Center sites as required in the Common Computing Environment project and where staffing allowed for it to be accomplished.

OIG Position

In order to achieve the management decision for this recommendation, we need to be provided a timeframe for completing a set of guidelines for providing supervisory reviews in offices where there are limited abilities to provide for segregation of duties.

FINDING NO. 8

Our review disclosed that the field offices had not always updated and/or tested their disaster recovery plans. Additionally, we found one site was not following the recommended procedure for offsite storage of system backups. Generally, field office personnel treated the update as more of a routine task to be performed on an annual basis rather than an opportunity to improve security. As a result, these field offices are increasing the potential for loss caused by a business interruption.

We found that one State used a disaster recovery plan that included some narrative detailing recovery methods. However, this plan has not been tested during the 3-year tenure of the current automation coordinator. The county office had not updated the security plan to reflect a change in the name of the offsite storage location. Additionally, we found that this State office was not following the recommended procedures for the offsite storage of system backups. Due to staffing shortages, the system backups were not being transported to the offsite storage facility at the recommended intervals.

Another State used a checklist, that did not include narrative, for the disaster recovery plan, which we found had not been tested for the last 2 years. The county office had a plan that had not been updated since 1997. We found that this office had received instructions that it only needed to update the plan if changes had occurred.

DM 3140-1 states that agencies should develop contingency plans to meet emergencies and ensure that the plans cover all critical processing. The plans should be reviewed annually and tested no less than annually. DM 3140-1 further states that offsite storage should be provided for information that is critical to program operations, that would be difficult to reconstitute, or that is required by law or custom to be current.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions, and (2) a plan to recover critical operations, should interruptions occur. These plans should consider the activities

performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises. In addition, all staff with service continuity responsibilities, such as backing up files, should be fully aware of the risks of not fulfilling these duties.

Although often referred to as disaster recovery plans these controls should address the entire range of potential disruptions to ensure service continuity. When controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data: Which can cause financial loss, expensive recovery efforts, and inaccurate or incomplete financial management information.

Additionally, we reviewed FSA's Federal Managers' Financial Integrity Act annual report for FY 2000 and determined that they had not reported any material weaknesses in internal controls in the IT area.

RECOMMENDATION NO. 10

Require those locations cited in this report to immediately update and/or test their contingency plans in accordance with existing policy.

FSA Response

FSA stated that it concurred with the recommendation and an IRM Notice would be developed addressing contingency plans and will require the plans to be submitted to FSA Kansas City to assure compliance.

OIG Position

We concur with the proposed actions and can achieve management decision upon receipt of the proposed timeframe for completing the contingency plans.

RECOMMENDATION NO. 11

Issue an IRM Notice requiring FSA State and county offices to update their contingency plans when any significant event occurred that affects the contingency plan, but not less than

annually. This Notice should also remind personnel of the importance of regularly scheduled transport of backups to the offsite storage facility.

FSA Response

FSA concurred with the recommendation and stated that this area would be addressed in the security handbook that is being developed as well as an IRM Notice this FY to address these specific weaknesses.

OIG Position

We concur with the proposed actions and can achieve management decision upon receipt of the specific timeframe(s) for completing the security handbook and IRM Notice.

RECOMMENDATION NO. 12

Make an Agency-level determination whether the conditions in this report represent a material internal control weakness and should be reported in the Agency's upcoming Federal

Managers Financial Integrity Act report.

FSA Response

FSA concurred with the recommendation and stated that they would forward and discuss the audit findings with the Chief Financial Officer (CFO) and assess the impact on the Federal Managers Financial Integrity Act report.

OIG Position

We concur with the proposed action and can achieve management decision when informed of the timeframe for accomplishing the FSA/CFO decision.

GENERAL COMMENTS

1. Filing of IT Security Training Certificates.

We noted that the method established for tracking the delivery of computer security awareness training could be improved. Our review of 76 randomly sampled Kansas City employees, from a population of 1,161, disclosed that 20 did not have IT Security Awareness Training Certificates on file.

EXHIBIT A – AUDITEE RESPONSE TO DRAFT REPORT



SEP 28 2001

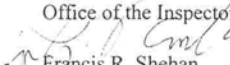
United States
Department of
Agriculture

Farm and Foreign
Agricultural
Service

Farm Service
Agency

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

TO: Dennis J. Gannon
Regional Inspector General for Audit
Office of the Inspector General

FROM:  Francis R. Shehan
Acting Director
Information Technology Services Division

ATTN: 03099-47-KC

SUBJECT: Comments on Official Draft of "Farm Service Agency/Commodity Credit Corporation–Security Over USDA Information Technology Resources"

The Farm Service Agency (FSA) is responding to the official draft audit report on the Farm Service Agency/Commodity Credit Corporation–Security Over Information Technology Resources.

The majority of security issues identified in this audit addresses weaknesses found in our Service Center State and county offices. Specific security concerns with individual State and county personnel were addressed immediately. Agency-wide recommendations will be addressed with Information Resources Management Security Notices as needed. Additionally, with the restructuring and consolidation of duties within the Common Computing Environment (CCE) Project between FSA, the Natural Resources Conservation Service (NRCS), and Rural Development (RD), many roles and responsibilities for security will be redefined and addressed which will directly resolve some of the Office of Inspector General (OIG) findings.

FSA appreciates the recommendations made by OIG and will address each potential weakness as required as to whether we concur or disagree and will identify the steps taken to resolve the concerns.

Finding No. 1 Network Security Assessments Revealed Vulnerabilities

OIG Recommendation No. 1: Take immediate action to eliminate the high-risk and medium-risk vulnerabilities identified by the scan reports.

FSA Response

We concur with the OIG recommendation. The FSA Security Offices worked closely with OIG during the time the scans were initiated as well as actively participated with OIG during the assessment reviews. Some of the high-risk and medium-risk

USDA is an Equal Opportunity Employer

vulnerabilities were corrected the day after they were found. In September 2000 FSA resolved the two high-risk vulnerabilities found in the Washington, DC (DC) office. In October 2000, FSA resolved the nine medium-risk vulnerabilities found in DC. This was done before the OIG Management Alert was issued. For the Kansas City, Missouri (KC) office, 35 of the 36 high-risk vulnerabilities were corrected within 2 months, the remaining vulnerability required research and was fixed on January 30. All 191 medium-risk vulnerabilities found in KC were researched and fixed as needed. The single high-risk vulnerability identified in the Iowa State Office was addressed within 5 days after being found on November 8, 2000. The five medium-risk vulnerabilities identified in the Iowa State Office were fixed by December 13, 2000. A memorandum to James Ebbitt of OIG dated December 6, 2000, addressed in detail FSA's progress in correcting these vulnerabilities.

The vast majority of the 898 low-risk vulnerabilities (809 out of 898) found in KC have been addressed and fixed. It is noted that many of these low-risk vulnerabilities were informational only, were redundant occurrences of the same vulnerability, and did not actually pose a threat to FSA information resources.

In addition, the KC FSA Security Office has procured the scanning tool Kane Security Analyzer for the DC and KC Novell systems. This is the same tool used by OIG to perform internal scans. FSA had also previously procured and deployed the Internet Security Systems (ISS) Internet Scanner tools used by OIG for Microsoft Windows NT and Windows 2000 systems to FSA KC and DC, the Risk Management Agency (RMA), and the Foreign Agricultural Service (FAS) networks. Training was attended by members of the security and telecommunications staffs on the certification of these scanner hardware and software tools.

NetWare Intruder Detection capabilities were enabled on the Novell network in KC immediately after this oversight was brought to our attention by OIG last year to address the specific OIG concern related to intrusion detection and to loginids not being suspended after a specific number of unsuccessful login attempts. The KC Telecommunications Division now searches for inactive Novell users on the first of every month. User accounts that have not logged in for 90 days are disabled. User accounts that have been disabled for an additional 30 days are removed.

OIG Recommendation No 2: Implement a policy to perform scans on a regular basis, and mitigate all weaknesses. Implement a policy of minimum security setting guidelines for Novell systems. Periodically assess the guidelines and determine if they remain appropriate.

FSA Response

We concur with the OIG recommendation. Effective March 1, FSA has initiated a security policy to perform scans every 3 months on the internal domains. Scans will soon be performed every month per a new Departmental policy. The scans are performed by the Information Security staff using ISS Internet Scanner tools. Kane Security software tools were procured to address the Novell platform and to produce reports of vulnerabilities and potential weaknesses. Reports of findings are forwarded to operations personnel for corrective action. Follow-up scans are initiated once the weaknesses have been corrected. In addition, as new servers are brought online, scans are performed to identify any potential weaknesses before the servers are operational.

OIG Recommendation No. 3: Immediately remove unnecessary accounts from the networks and implement a system of controls that prevents the creation and retention of unnecessary accounts.

FSA Response

We concur with the OIG recommendation. When FSA employees leave the Agency, they complete a clearance form. An AD-1106 form, "Final FFAS Clearance Report" is used in DC; a KC-256, "Final Salary Payment and Clearance Form" is used in KC. The FSA Security staff has reviewed this internal process to make sure it is completed in a timely manner. Per FFAS policy (Notice IRM-307, "Information Systems Security Program") Local Area Network (LAN) Administrators are responsible for automatically suspending user identification codes that have been inactive for 30 calendar days

In addition, Inactive User Procedures for the FSA network have been developed as a backup to assure unauthorized users are deleted from the networks. In KC, the Telecommunications Division searches for inactive Novell users on the first of every month. User accounts that have not logged in for 90 days are disabled. User accounts that have been disabled for an additional 30 days are removed. In DC, the FSA LAN Staff searches for inactive Novell users every 2 to 3 months for user accounts that have not been used for 6 months. Because some DC users are sent on temporary assignments, user accounts may be unused for a few months.

Finding No. 2 Local Controls Did Not Ensure Restricted System Usage

OIG Recommendation No. 4: Issue an IRM Notice to all FSA employees reminding them of their responsibilities to protect sensitive program data. The notice should emphasize how the sharing of passwords and failure to protect sensitive data can have an adverse impact on USDA programs and personnel. The notice should also require each systems administrator to review the list of current userids, reconcile this to active employees, and delete userids for any inactive employees. Additionally, the notice should remind systems administrators of their ongoing responsibility to ensure that userids are deleted as soon as an employee is separated from service with FSA.

FSA Response

We concur with the OIG recommendation. The Security staff is developing a security handbook for all FSA employees that will be ready for distribution by the second quarter of 2002. In the meantime, we will issue an IRM Security Notice this fiscal year to address the weaknesses identified in this finding and to address general security "best practices." We believe these weaknesses are limited in scope to specific State and county offices since the majority of our field offices are fully aware of their security responsibilities and are reminded periodically as required by the Department, as well as through the annual Computer Security Awareness training program. FSA has developed a comprehensive security awareness training program that addresses common security weaknesses and outlines security best practices concepts for an effective security posture. FSA is reviewing a web-based interactive training program for fiscal year 2002 (FY 2002). This web-based training program will provide the automatic completion of training certificates and notification to the security staff upon completion of the training.

Please note that USDA Departmental Regulation (DR) 3300-1 allows "limited personal use" of the Internet by FFAS employees and contractors. It supersedes the provisions of DR 3140-2 (mentioned in the audit report) that the Internet is for official USDA business only. However, certain activities (such as downloading or viewing pornography) are still prohibited.

Finding No. 3 Physical Controls Do Not Effectively Restrict Access to Servers

OIG Recommendations No. 5: Keep servers and related materials within secured environments and limit access to systems administrators and their alternates. If access is required by others, adequate monitoring should be provided. Ensure that available keyboard-locking features are utilized.

FSA Response

We concur with OIG's recommendation. Our DC and KC Headquarter network and telecommunications offices are fully secured and access is restricted according to USDA Policy. Recently the Office of the Chief Information Officer (OCIO) Cyber Security Office performed an on-site physical security assessment in KC and made additional recommendations that FSA will address as funding is made available. We recognize the majority of the weaknesses found in this finding are directed to specific field offices. Again, with the implementation of the CCE project, servers and LAN/WAN/Voice hardware will be stored and locked in specified security rooms. FSA will make every attempt to enforce this policy in the future with the cooperation of the Service Center partner agencies (NRCS and RD). As funds are made available, FSA will look at the feasibility and cost benefits of redesigning and creating separately controlled computer server rooms and "web farm" rooms in Government leased space.

Forced Screen Savers and timeouts for users for the FSA network are being implemented. In addition, this issue is being implemented on the CCE platform.

Finding No. 4 Internet Access Not Suspended During Disciplinary Actions

OIG Recommendation No. 6: Institute a procedure that allows the security staff to immediately restrict a user's Internet access when they become aware that a user has been visiting websites deemed inappropriate by USDA management.

FSA Response

FSA cannot implement this recommendation at this time. This is a very complex issue with no simple solution. Only the FSA Kansas City and St. Louis offices have a proxy server in place that requires employees to sign-on to the Internet using a userid and password so we can track and block access. This function is not available in Washington, DC; State offices; nor our field office Service Centers.

FSA follows a personnel process for KC employees that has been in place for several years for investigations. It involves the offending employee's immediate supervisor, a Personnel Relations Specialist, and a Security Office staff member. Employees are considered innocent until proven guilty. Once it has been determined that the charges against an employee have been substantiated and proved, Human Resources has the ability to notify the Security Office to suspend the Internet access of the employee for a specific time period, if warranted, along with harsher penalties including suspension and removal. We do not consider this an issue within the KC Office.

Suspending employees' Internet access in the field and DC office is a more complex technical issue. DC, the field office Service Centers, and State offices are not configured to control access to the Internet through a central proxy server where access could be centrally managed, and there are no plans at this time for the CCE environment to move in that direction. All of the vulnerabilities in the OIG audit were directed to specific field office sites where access is not being monitored. To shut off Internet access would require removing the web browser connection from the workstation.

Access for field office Service Centers would have to be managed at the OCIO firewall for this type of solution to be implemented, which is not in our control. OCIO is aware of this problem and is looking at providing some type of access monitoring tools at the OCIO device stack in the next fiscal year. Therefore, FSA cannot comply with this recommendation at this time, but will continue to make sure that FSA employees are made aware this is an offense that will not be tolerated.

Finding No. 5 Required Risk Assessments Were Not Performed

OIG Recommendation No. 7: Complete the risk assessments as soon as possible and implement a system of controls to ensure that risk assessments are completed on a yearly basis, or as system changes demand.

FSA Response

We concur with the OIG recommendation. Our number one priority is to develop, test, implement and support ongoing Farm Programs mandated by Congress within specific time frames. With limited resources, FSA has had to make several complex decisions on prioritizing high-ranking assignments. In addition, FSA has endured major budget cuts and staffing reductions that have limited the availability of funds for contractor support to perform risk assessments this fiscal year.

The Security Office has prioritized the Sensitive System Applications FSA supports and maintains, and will perform a risk assessment on the 12 major sensitive systems for fiscal year 2001. FSA has procured a software risk assessment package (Cobra) to assist us in performing these risk assessments. Funding has been included in FY 2002 and 2003 to address additional risk assessments for the remaining systems.

In addition, FSA is working closely with the OCIO Cyber Security Office and other USDA agency representatives to develop a risk assessment checklist that is platform-specific. Currently checklists for Telecommunications, the Windows 2000 and NT servers and workstations, and UNIX have been developed. Training was held in DC and KC on the use of these checklists. A draft checklist has been developed for the IBM AS/400 platform. Once the checklists are finalized and training provided, system application developers will be able to perform self-assessments on existing and new applications which will greatly reduce contractor funds for performing these types of required assessments.

Finding No. 6 Security Responsibilities Not Clearly Established

OIG Recommendation No. 8: Issue an IRM Notice requiring the owners of all sensitive systems to ensure that the next update of their security plan includes a documented security management structure.

FSA Response

We disagree with your recommendation but agree with the need. OCIO requested the 2001 annual system security plans contained a new structured format that addressed among a multitude of security questions, the security management structure. Note: Security responsibilities for the system mentioned in the report (MAS) have been assigned to appropriate FSA DC security and system development staff.

FSA completed 113 major support security plans following the new format and the remaining applications will be addressed in this new format for FY-2002. FSA no longer considers this specific weakness a major security issue and will continue to review all plans annually to assure this information is included in the security plans. We will also address this in the security handbook.

Finding No. 7 (Inadequate separation of duties at some field locations)

OIG Recommendation No. 9: In conjunction with the implementation of the LAN/WAN/Voice project, develop a set of guidelines for providing supervisory review in offices where there is limited ability for segregation of duties.

FSA Response

We concur with the OIG recommendation. FSA has experienced a major reduction in staffing over the past six years, and especially in our field office service centers. We are aware of the "separation of duties" principal for security and will address these

concerns in our co-located service center sites as required in the CCE project and where staffing allows for this to be accomplished.

Finding No. 8 (Field Offices had not always updated and/or tested their disaster recovery plans)

OIG Recommendation No. 10: Require those locations cited in this report to immediately update and/or test their contingency plans in accordance with existing policy.

FSA Response

We concur with the OIG recommendation. FSA as an Agency participated in annual National Information Technology Center (NITC) "Hot Site" testing programs and just completed another hot site test in July 2001. An IRM Notice will be developed and issued addressing contingency plans and will require the plans be submitted to FSA Kansas City office to assure compliance. Service Centers are extremely busy which limits actual testing of contingency plans. FSA cannot afford to shut down actual offices during the day to test actual disaster plans. We will review this process and try to identify a potential solution that is acceptable to all business partners without disruption to our customers.

OIG Recommendation No. 11: Issue an IRM Notice requiring FSA State and county offices to update their contingency plans when any significant event occurs that affects the contingency plan, but not less than annually. This Notice should also remind personnel of the importance of regularly scheduled transport of backups to the off-site storage facility.

FSA Response

We concur with the OIG recommendation. Our Security Office will address this issue in the security handbook that is being developed and will address this issue in an IRM Notice this fiscal year to address these specific weaknesses.

OIG Recommendation No. 12: Make an Agency-level determination whether the conditions in this report represent a material internal control weakness and should be reported in the Agency's upcoming Federal Managers Financial Integrity Act report.

FSA Response

We concur with the OIG recommendation. FSA will forward our responses to this specific audit to the CFO and discuss the findings in detail so as to assess the impact on the Federal Managers Financial Integrity Act report.

OIG General Comments: OIG noted that the method established for tracking the delivery of computer security awareness training could be improved.

FSA Response

We concur with the OIG recommendation. FSA is reviewing a web-based interactive training program for FY-2002. It would include automatic completion of training certificates and notification of the security staff and personnel office upon completion of the training.

For More Information

Thank you for providing FSA with the opportunity to comment on the draft audit. If you have questions or need any more information, please contact me at (202) 720-5320 or contact FSA's Information Systems Security Program Manager, Brian J. Davies, at (202) 720-2419.

ABBREVIATIONS

ADP - Automatic Data Processing

CCC - Commodity Credit Corporation

CFO – Chief Financial Officer

CO - County Office

CORP - County Office Review Program

DM - Departmental Manual

DR - Departmental Regulations

FSA - Farm Service Agency

FY - Fiscal Year

ID - Identification Number

IRM - Information Resource Management

IT - Information Technology

LAN - Local Area Network

OCIO - Office of the Chief Information Officer

OMB - Office of Management and Budget

SO - State Office

TCP/IP - Transmission Control Protocol/Internet Protocol

USDA - United States Department of Agriculture

WAN - Wide Area Network

