FARM CREDIT ADMINISTRATION

INDEPENDENT ACCOUNTANT'S REPORT
ON AGREED-UPON PROCEDURES:
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT EVALUATION

For the Year Ending September 30, 2005

HARPER, RAINS, KNIGHT & COMPANY, P.A.
CERTIFIED PUBLIC ACCOUNTANTS
RIDGELAND, MISSISSIPPI

Table of Contents

Executive Summary

This report includes the agreed-upon procedures and the results from applying those procedures, specified by the Farm Credit Administration's (FCA) Office of Inspector General, solely to assist with the annual evaluation of FCA's security program and practices and reporting requirements of the Federal Information Security Management Act (FISMA) submitted to the Office of Management and Budget (OMB).

FCA is an independent agency in the executive branch of the U. S. Government. It is responsible for the regulation and examination of the banks, associations, and related entities that collectively comprise what is known as the Farm Credit System (System). FCA promulgates regulations to implement the Farm Credit Act of 1971, and examines System institutions for compliance with the Act, regulations, and safe and sound banking practices.

The system evaluations were performed following guidance issued by the National Institute of Standards and Technology (NIST) Self-assessment guide. The Office of Inspector General, determined the critical elements that represent essential tasks for establishing compliance with FISMA, and the guidelines issued by OMB, the Government Accountability Office (GAO), the Chief Information Officer (CIO) Council, and applicable NIST guidance for each control category, including:

- documented security policies;
- documented security procedures;
- implemented security procedures and controls;
- tested and reviewed security procedures and controls; and
- fully integrated security procedures and controls.

No exceptions were noted during the performance of the agreed-upon procedures for determining FCA's compliance with FISMA.

Our procedures were performed in accordance with attestation standards established by the American Institute of Certified Public Accountants and *Government Auditing Standards* issued by the Comptroller General of the United States.

HRK

HARPER, RAINS, KNIGHT
& COMPANY

Certified Public Accountants
A Professional Association

Independent Accountant's Report on Applying Agreed-Upon Procedures

The Inspector General
Farm Credit Administration

We have performed the procedures outlined in Exhibit A that were agreed to by the Farm Credit Administration's (FCA or Agency) Office of Inspector General, solely to assist with the annual evaluation of FCA's security program and practices and reporting requirements of the Federal Information Security Management Act (FISMA) submitted to OMB. FCA's management is responsible for documented security policies, documented security procedures, implemented security procedures and controls, tested and reviewed security procedures and controls, and fully integrated security procedures and controls for its mission critical systems listed below. This engagement to apply agreed-upon procedures was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants and *Government Auditing Standards* issued by the Comptroller General of the United States. The sufficiency of these procedures is solely the responsibility of the Inspector General of FCA. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

The agreed-upon procedures and related results of procedures are included in the attached Exhibit A. The OMB FISMA Reporting Template, a required document of these agreed-upon procedures, is included in Exhibit B.

Our procedures covered the agency systems included in the attached Appendix A.

We were not engaged to, and did not, perform an examination or a review, the objective of which would be the expression of an opinion on the FCA's security program and practices. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

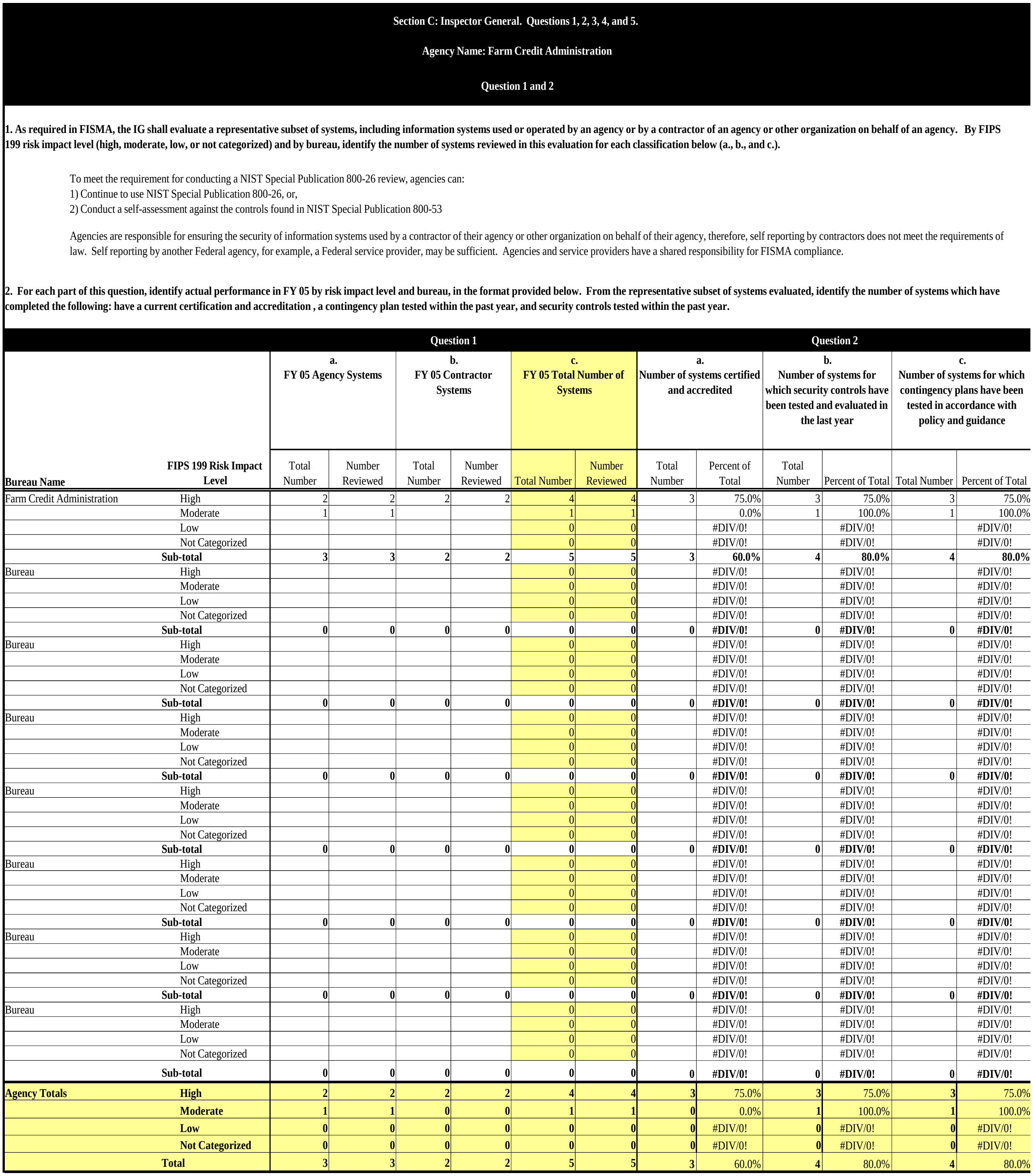
This report is intended solely for the information and use of the FCA Inspector General and is not intended to be and should not be used by anyone other than the specified party. This report should not be used by those who have not agreed to the procedures and taken responsibility for the sufficiency of the procedures for their purposes.

Harper, Rains, Knight & Company, P.A.

September 20, 2005

Pages 4 through 7 removed

Exhibit B – OMB FISMA Reporting Template



Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: Farm Credit Administration

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						**Question 2**					
		a. FY 05 Agency Systems		**b. FY 05 Contractor Systems**		**c. FY 05 Total Number of Systems**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and evaluated in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Farm Credit Administration	High	2	2	2	2	4	4	3	75.0%	3	75.0%	3	75.0%
	Moderate	1	1			1	1		0.0%	1	100.0%	1	100.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**3**	**3**	**2**	**2**	**5**	**5**	**3**	**60.0%**	**4**	**80.0%**	**4**	**80.0%**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Agency Totals	**High**	2	2	2	2	4	4	3	75.0%	3	75.0%	3	75.0%
	Moderate	1	1	0	0	1	1	0	0.0%	1	100.0%	1	100.0%
	Low	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
	Not Categorized	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
	Total	3	3	2	2	5	5	3	60.0%	4	80.0%	4	80.0%

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Almost Always, for example, approximately 96-100% of the time
3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 96-100% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes
Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time		
4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Almost Always, for example, approximately 96-100% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Almost Always, for example, approximately 96-100% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 96-100% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time
Comments:		
Question 5		
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .		
	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Good
Comments: In FY 2005, FCA contracted with Pinnacle CSI to perform an assessment of FCA's certification and accreditation policies and procedures to provide management with a level of confidence that their systems and applications operate effectively and that the proper policies and procedures to mitigate risks to an acceptable level are in place. In addition, Pinnacle CSI performed a Certification and Accreditation (C&A) on FCA's Windows 2003 System in accordance with NIST Special Publication 800-37. FCA reviews third party documents (e.g. SAS 70 reports) for evidence of C&A's on their contractor systems. During our evaluation FCA indicated they plan to conduct formal C&A's on two more of their systems in FY 2006. In FY 2005 FCA's C&A policies, procedures, and guidelines were updated to adhere to NIST Special Publication 800-37.		

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name: Farm Credit Administration

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	N/A		
HP-UX	N/A		
Linux	N/A		
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Other. Specify:	N/A		

Comments:

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments:

	Question 8	
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Almost Always, or approximately 96-100% of employees have sufficient training
	Question 9	
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

Appendix A – Agency Systems

Our procedures were applied to the following agency systems.

1) Major Applications

a. Federal Financial System (FFS)

- FFS is the major application that supports all FCA core accounting functions including budget execution, accounts payable, disbursements, purchasing, travel, accounts receivable, general ledger, document tracking, project cost accounting, and external reporting. FFS is a mainframe computer financial management system. FFS is processed by the United States Geological Survey (USGS)/National Business Center (NBC), and American Management Systems, Inc. (AMS). The FFS software is owned and maintained by AMS. AMS is responsible for providing development activities including regular upgrades, fixes, and requested enhancements to maintain the core FFS software. NBC personnel are responsible for defining and developing processes to retrieve or receive data from external sources to develop corresponding programs that enable FFS to load the data accordingly. FCA’s FFS security administrator, located in the Chief Financial Office is responsible for managing security access control to the FFS agency application. FFS was placed in production in June 2001.

b. Payroll Services from National Finance Center (NFC)

- USDA's NFC located in New Orleans, Louisiana provides the Personnel/Payroll System (PPS) to FCA. NFC provides distributed application and telecommunications support for the remote site located in McLean, Virginia. NFC developed a "master security plan" for the general support system in New Orleans. FCA's Chief Administrative Office maintains a security plan for the remote system at FCA that incorporates provisions of the master security plan.

c. Consolidated Reporting System (CRS)

CRS is a major application that supports FCA operations. CRS is an Oracle relational database containing financial and statistical information on active and inactive System institutions. CRS contains three distinct subsystems that are Call Report, Loan Account Reporting System (LARS), and Web-based CRS Reports:

- Call Report is comprised of financial information including a statement of condition, statement of income, and supporting schedules that is collected quarterly from the System institutions. Call Report subsystem is monitored, analyzed, and assessed by FCA examiners and financial analysts to ensure that the integrity and confidentiality of financial data are maintained.

- LARS database contains specific loans of System lender institutions. Such institutions submit the data quarterly to FCA via diskette or zip file. The loan data are loaded using SQLLoader, and are then verified and validated by FCA personnel.

- Web-based CRS Reports is an FCA developed application using the JavaScript front-end interface and an Oracle database back-end application. The reports are built using e-Reporting Suite, and are available on FCA's Web site. The Freedom of Information Act (FOIA) versions of the reports are available to the public. The non-FOIA versions of the reports are available to users who are authorized to view their institution data.

d. Lotus Domino (Notes)

- The Notes application is a database system software owned and maintained by FCA. The application supports the daily administrative tasks including e-mail, group discussion, calendaring and scheduling, database management, forms, and workflow of FCA.

2) General Support Systems

a. Windows 2003 Network

- Windows 2003 is an operating system or the core program of a computer that allows the other programs and applications to operate. Windows 2003 is fully integrated with networking capabilities and was designed for client/server computing to facilitate user workstation connections to servers and the sharing of information and services among computers.

- Windows 2003 Server is the primary operating system installed on substantially all servers in the FCA network. Additionally, Windows 2000 and XP are installed on agency laptop and desktop computers where they function as a client to the FCA network as well as a stand-alone operating system for the client hardware. Through Windows 2000/XP, users can access network services such as file servers, e-mail, the Internet, applications and shared hardware such as printers.

Appendix B – Acronyms and Abbreviations

AMS	American Management Systems, Inc.
C&A	Certification and Accreditation
CIO	Chief Information Officer
COGCON	Continuity of Government Condition System
CRS	Consolidated Reporting System
FCA	Farm Credit Administration
FFS	Federal Financial System
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	Government Accountability Office
IT	Information Technology
LARS	Loan Account Reporting System
NBC	National Business Center
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCAO	Office of the Chief Administrative Officer
OCFO	Office of the Chief Financial Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestone
PPS	Personnel/Payroll System
System	Farm Credit System
US-CERT	United States Computer Emergency Readiness Team
USGS	United States Geological Survey