FARM CREDIT ADMINISTRATION

INDEPENDENT ACCOUNTANTS' REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT EVALUATION

For the Year Ending September 30, 2006

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

Table of Contents

Executive Summary

The Federal Information Security Management Act of 2002 (FISMA) requires agency program officials, Chief Information Officers (CIO), and Inspector Generals (IGs) to conduct annual reviews of the agency's information security program and report the results to the Office of Management and Budget (OMB). OMB issues annual reporting guidance in the form of a memorandum to the respective parties. Under contract with the Farm Credit Administration's (FCA or the Agency) Officer of Inspector General we performed an evaluation of the Agency's security program and practices, solely to assist the IG with the annual evaluation and reporting to OMB.

This report includes the objective, scope, methodology, and results of our evaluation to assist with reporting requirements of the FISMA submitted to OMB.

Our evaluation included determination of the critical elements which represent tasks that are essential for establishing compliance with FISMA, and guidelines issued by OMB, the Government Accountability Office (GAO), the Chief Information Officers (CIO) Council, and the National Institute of Science and Technology (NIST) 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.

Our evaluation was performed in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Our evaluation did not reveal any information security control matters that we deemed to be significant deficiencies that must be reported under FISMA.

HARPER, RAINS, KNIGHT & COMPANY
Certified Public Accountants
A Professional Association

Independent Accountants' Report

Mr. Carl Clinefelter,
Inspector General
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Harper, Rains, Knight & Company, P.A. conducted an evaluation of the Farm Credit Administration's security program and practices for compliance with requirements of the Federal Information Security Management Act of 2002 (FISMA).

We conducted the evaluation solely to assist the Office of Inspector General with the annual evaluation and reporting to Office of Management and Budget (OMB) of the Farm Credit Administration's security program and practices.

Our evaluation did not reveal any information security control matters that we deemed to be significant deficiencies that must be reported under OMB FISMA requirements, see Appendix B.

We conducted our evaluation in accordance *Government Auditing Standards*, issued by the Comptroller General of the United States, for performance audits. Our objective, scope, methodology, and results are detailed in Appendix A.

We were not engaged to, and did not perform an audit of Farm Credit Administration's security program and practices, the objective of which would be the expression of an opinion on such information. Accordingly, we do not express such an opinion.

This report is intended solely for the information and use of the Farm Credit Administration's Office of Inspector General, Office of Management Services, and Board of Directors, and is not intended to be, and should not be, used by anyone other then these specified parties.

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

Harper, Rains, Knight & Company, P.A.
September 29, 2006

APPENDIX A

Objective

The objective of the evaluation was to (1) assist the IG in responding to reporting requirements issued by OMB and (2) verify and test the Agency's information system security program and practices.

Scope

Our evaluation covered FCA's agency owned and contractor operated information systems of record as of September 30, 2006. FCA is a single program agency with five mission critical systems. Mission critical systems are defined as any telecommunications or information system used or operated by an agency or by a contractor of an agency, or organization on behalf of an agency that processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

In accordance with FISMA and OMB's implementation guidance, we evaluated the following mission critical systems.

1. Major Applications

   a. Oracle Federal Financials from Bureau of the Public Debt (BPD)

      Oracle Federal Financials is the major application used at BPD 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. The Administrative Resource Center (ARC) operates Oracle version 11i, with the Oracle 9i database, which runs on the ARC subnet and accesses data in the ARC Demilitarized Zone (DMZ) using Linux as its operating system. ORACLE uses a two-tier web-based infrastructure with a front-end Internet user interface and a database residing on the secure network. The application (web-applet) accesses the database IP to IP on a specified port that is defined in the Access Control List. External Internet access is via a SSL 128-bit encrypted connection. External security is also provided by OIT through a PIX firewall and router Access Control Lists. ARC also uses a report writer package called Discover that provides users with the ability to create their own ad hoc reports for query purposes.

   b. Payroll Services from National Finance Center (NFC)

      The National Finance Center (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 Office of Management Services (OMS) 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 Farm Credit 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. 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)

Lotus Domino (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. Mission Critical General Support Systems

a. Windows Operating System

Windows is an operating system or the core program of a computer that allows the other programs and applications to operate. Windows 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 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.

Methodology

The system evaluations were performed in accordance with the NIST assessment guide. The Office of Inspector General, assisted by Harper, Rains, Knight & Company, P.A., the independent evaluator, determined the critical elements that represent essential tasks for establishing compliance with FISMA, and the guidelines issued by OMB, GAO, CIO Council, and NIST 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.

For each control category, the evaluator determined the associated objectives, risks, and critical activities, as well as related control techniques and evaluation concerns specific to FCA's information technology environment.

The evaluation was conducted in accordance with the requirements and criteria found in GAO's FISCAM, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," current NIST guidance, and the CIO Council Framework. We used this information to evaluate FCA's practices and addressed the above five control areas to be considered in determining compliance with FISMA. For each critical element, the evaluator made a summary determination as to the effectiveness of FCA's related controls. If the controls for one or more of each category's critical elements were found ineffective, then the controls for the entire category are not likely to be effective. The evaluator exercised its professional judgment in making such determinations.

The evaluation focused on the actual performance of the Agency's security program and practices and not on how the Agency measures its performance in its own annual evaluations. The Agency's security controls were evaluated for programs and practices including testing the effectiveness of security controls for Agency systems or a subset of systems as required. The evaluator performed FISMA evaluations in accordance with Federal guidance, e.g., NIST Self-Assessment Guide for Information Technology Systems.

The evaluation procedures were divided into three "classes" and further divided into seventeen "families" as identified in NIST Special Publication 800-53:

- **Management**
    - Risk assessment – Controls in place to categorize information systems in accordance with FIPS 199, to assess the potential impact of unauthorized access, and to update the risk assessment regularly.
    - Planning – Controls in place to ensure a security plan is in place and to ensure the plan is readily available, updated regularly, and tested.

- System and services acquisition – Controls in place to allocate resources during capital budgeting, using a system development life cycle, and to implement the information system using security engineering principles.
- Certification, accreditation, and security awareness – Controls in place to certify and accredit information systems and interconnected systems and to develop and update the plan of action and milestones (POA&M).

- **Operational**
  - Personnel security – Controls in place for employee screening, handling of terminated employees, and compliance failure sanctions.
  - Physical and environmental control – Controls in place for physical access to the building and areas sensitive to information systems, visitor access, and preventative measures for physical damage to information systems components.
  - Contingency planning – Controls in place for training, testing, and reviews of all contingency plans as well as providing alternative storage and processing sites.
  - Configuration management – Controls in place to document configuration information, to monitor changes, and to restrict access to information systems.
  - Maintenance – Controls in place to control remote diagnostic activities, restrict personnel allowed to perform maintenance, keep maintenance contracts, and have spare parts on hand.
  - System and information integrity – Controls in place to correct system flaws, monitor systems events, and protect against unauthorized changes.
  - Media protection – Controls in place to ensure only authorized personnel have access to sensitive media, appropriately mark and store media, and sanitize media when it is no longer needed.
  - Incident response – Controls and procedures in place to train personnel in their roles, test the response capability, and properly document incidents.
  - Awareness and training – Controls in place to implement security awareness and training for all employees including managers and to monitor training and stay up to date with current technology and security practices.

- **Technical**
  - Identification and authentication – Controls in place to identify and authenticate users of information systems, to authenticate devices on information system networks, and to mange users of information systems.
  - Access control – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
  - Audit and accountability – Controls in place to generate, review, and protect audit data and reports.
  - Systems and communication protection – Controls in place to separate user functionality from management, to protect against internet attacks, and to establish trusted communication paths between the user and the system.

Results

Our procedures did not reveal any information system security control matters that we deemed to be significant deficiencies that must reported under FISMA.

Risk assessment

FCA has controls in place to categorize information systems in accordance with FIPS 199, to assess the potential impact of unauthorized access, and to update the risk assessment, at least annually. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA categorizes information systems in accordance with FIPS 199. We found FCA conducts annual risk assessments over their information systems. We found FCA has a Continuity of Operations Plan (COOP) in place and that it is reviewed annually. We found FCA has a system in place to track general security notifications and assess potential impact.

Planning

FCA has controls in place to ensure a security plan is in place and to ensure the plan is readily available, updated regularly, and tested. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA has incorporated its security plans into the COOP plan. We found the security plans are reviewed annually and revised when appropriate. We found FCA provides training to employees on the expectations of using their information systems. We founds FCA tests the impact of changes prior to implementing changes on their information systems.

System and services acquisition

FCA has controls in place to allocate resources during capital budgeting, using a system development life cycle, and to implement the information system using security engineering principles, where applicable. We found FCA has policies and procedures in place and that they are periodically reviewed. We found the Information Resources Management (IRM) plan outlines and budgets for future information technology needs. We found FCA applies a system development life cycle to their information systems. We found security is considered during FCA's information system planning and acquisition process. We found FCA tracks licenses and installations to comply with software usage restrictions. We found FCA does not allow software to be downloaded and installed unless it is supplied by FCA or approved on an individual basis. We found that FCA designs and implements information systems using security engineering principles.

Certification, accreditation, and security awareness

FCA has controls in place to certify and accredit information systems and interconnected systems and to develop and update the plan of action and milestones (POA&M). We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA

conducts assessments of security controls in information systems annually to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome. We found FCA authorizes all interconnections to other information systems outside the accreditation boundary and monitors/controls the information system interconnects on an ongoing basis. We found FCA develops and updates POA&Ms and reports POA&Ms on a quarterly basis. We found FCA has a policy to perform C&A on its information systems every three years or when significant information systems changes occur.

Personnel Security

FCA has controls in place for employee screening, handling of terminated employees, and compliance failure sanctions. We found FCA has policies and procedures in place and that they are periodically reviewed. We found each FCA Position Description (PD) has a "Position Sensitivity" indicator. We found FCA employees are not granted access to information systems without a sponsor's approval. We found when an employee is terminated, quits, or retires FCA requires the individual to complete a separation checklist. We found FCA requires new hires and contractors to sign FCA's Computer Security Program Employee Certification, which declares they have read FCA's Computer Security Program, Policies, and Procedures Manual.

Physical and environmental protection

FCA has controls in place for physical access to the building and areas sensitive to information systems, visitor access, and preventive measures for physical damage to information systems components. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA issues identification badges to all personnel, including contractors. We found FCA controls all entry point via either guarded entry or Kastle Key access. We found a visitor access log is maintained at the front desk. We found FCA's information system distribution and transmission lines are run through the secured computer room. We found all visitors must be escorted in to the computer room by an FCA employee. We found FCA maintains an uninterruptible power supply for the secured computer room. We found FCA implements redundant HVAC units in the controlled computer room to control the temperature. We found FCA keeps track of computers through the Property Management Tracking System (PMTS).

Contingency planning

FCA has controls in place for training, testing, and reviews all contingency plans as well as providing alternative storage and processing sites. We found FCA has policies and procedures in place and that they are periodically reviewed. We found responsible FCA personnel have been trained as to their responsibilities in the event of an emergency and the COOP has been regularly tested via the COGCON exercises. We found the COOP is reviewed annually and updated as required. We found FCA has an emergency operations center that serves as its alternate processing site and the resumption of information system operations for mission critical functions when the primary processing capabilities are unavailable. We found FCA runs backups of user and systems information daily (incremental) and weekly (full).

Configuration management

FCA has controls in place to document configuration information, to monitor changes, and to restrict access to information systems. We found FCA has policies and procedures in place and that they are periodically reviewed. We found information system changes are tested and monitored after being put in production. We found FCA has established configuration setting for information technology, has set default access as none, and enforces configuration settings in all components of the information system.

Maintenance

FCA has controls in place to control remote diagnostic activities, restrict personnel allowed to perform maintenance, keep maintenance contracts, and have spare parts on hand. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA does not have vendors perform preventative maintenance on servers. We found FCA runs HP/Compaq Insight System Manager, which monitors the health of servers and reports on problems via email. We found FCA controls and monitors maintenance on FCA laptops. We found FCA has a contract with a four hour response time to repair the servers.

System and information integrity

FCA has controls in place to correct system flaws, monitor system events, and protect against unauthorized changes. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA has virus protection software installed and it updates automatically. We found FCA continuously monitors the information systems to detect attacks and prevent unauthorized use. We found FCA participates in the US-CERT program. We found FCA restricts which personnel can make changes to the information systems. We found FCA applications have edit checks built in to ensure data integrity.

Media protection

FCA has controls in place to ensure only authorized personnel have access to sensitive media, mark and store media, and sanitize media when it is no longer needed. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA restricts user access to drives and applications. We found FCA labels do not indicate what is stored on the media and that back up tapes are stored in a safe. We found FCA controls the system media and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

Incident response

FCA has controls and procedures in place to train personnel in their roles, test the response capability, and properly document incidents. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA trains their employees to respond to incidents. We found FCA continually monitors for intrusions and documents and investigates unusual activity.

Awareness and training

FCA has controls in place to implement security awareness and training for all employees including managers and to monitor training and stay up to date with current technology and security practices. We found FCA has policies and procedures in place and they are periodically reviewed. We found FCA requires all employees to complete an annual Information Technology Security Awareness training. We found FCA documents annual security training activities through FCA News Flash emails.

Identification and authentication

FCA has controls in place to identify and authenticate users of information systems, to authenticate devices on information system networks, and to manage users of information systems. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA users must be authenticated before accessing any resource not publicly available on the internet. We found the encryption used on the website to access FCA information, SSL, meets federal standards.

Access control

FCA has controls that limit and monitor access to computer resources to protect against unauthorized modification, loss, and disclosure. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA deactivates accounts after a defined period of inactivity and passwords must be changed periodically. We found FCA uses least privileged access. We found FCA enforces segregation of duties through assigned authorization. We found FCA locks computers after three consecutive unsuccessful login attempts. We found that FCA does not permit employees to use personally owned equipment to access the FCA network.

Audit and accountability

FCA has controls in place to generate, review, and protect audit data and reports. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA information systems keep logs which provide an audit trail. We found FCA is notified via email of suspicious events in addition to the event being recorded in the log. We found FCA has the ability to produce audit trail reports from the firewall and intrusion detection system. We found FCA's event/audit logs include time stamps. We found FCA audit log information is restricted to the information technology personnel.

System and communications protection

FCA has controls in place to separate user functionality from management, to protect against internet attacks, and to establish trusted communication paths between the user and the system. We found FCA has policies and procedures in place and that they are periodically reviewed. We found FCA enforces access controls in order to limit personnel who use the system from personnel who manage the system. We found FCA has controls in place to limit the effects of

common attacks, including denial of service attacks. We found FCA has controls in place to ensure high priority processes, such as virus scans, have access to needed resources. We found FCA information is transmitted by secure means such as SSL. We found FCA terminates remote connections after 30 minutes of inactivity. We found FCA separates FOIA information from private information on the website.

APPENDIX B

OMB FISMA Reporting Template

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

Agency Name:

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 over the past fiscal year 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. Agency Systems		b. Contractor Systems		c. 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	1	50.0%	2	100.0%	2	100.0%
	Moderate	1	1	2	2	3	3	2	66.7%	3	100.0%	3	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%**	**5**	**100.0%**	**5**	**100.0%**
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**	**0**	**0**	**2**	**2**	**1**	50.0%	**2**	100.0%	**2**	100.0%
	Moderate	**1**	**1**	**2**	**2**	**3**	**3**	**2**	66.7%	**3**	100.0%	**3**	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%	**5**	100.0%	**5**	100.0%

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 and/or NIST 800-53 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.1.	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.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: N/A Missing Contractor Systems: N/A
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 2006, FCA planned an independent contract review to provide an independent certification and accreditation (C&A) on their remaining two agency systems. Due to a transfer of procurement services to the Bureau of Public Debt, the contract was not finalized in time to complete the C&A's in FY 2006. The C&A's will be performed in the first quarter of FY 2007.		

Section B: Inspector General. Question 6, 7, 8, and 9. Agency Name: 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	N/A	No	
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	N/A	No	
HP-UX	N/A	No	
Linux	N/A	No	
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	No	
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 C

Acronyms and Abbreviations

ARC	Administrative Resource Center
BPD	Bureau of Public Debt, Oracle Federal Financials
C&A	Certification and Accreditation
CIO	Chief Information Officer
COGCON	Continuity of Government Condition
COOP	Continuity of Operations Plan
CRS	Consolidated Reporting System
DMZ	Demilitarized Zone
FCA/Agency	Farm Credit Administration
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	Government Accountability Office
HP	Hewlett Packard
HVAC	Heating Ventilating and Air Conditioning
IP	Internet Protocol
IRM	Information Resource Management
IT	Information Technology
LARS	Loan Account Reporting System
NFC	National Finance Center
NIST	National Institute of Science and Technology
OCFO	Office of the Chief Financial Officer
OIG/IG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OMS	Office of Management Services
PD	Position Description
PMTS	Property Management Tracking System
POA&M	Plan of Action and Milestone
PPS	Personnel/Payroll System
SSL	Secure Socket Layer
System	Farm Credit System
US-CERT	United States Computer Emergency Readiness Team