FARM CREDIT ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 EVALUATION

For the Fiscal Year Ending September 30, 2007

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

Table of Contents

Executive Summary

Under the Federal Information Security Management Act of 2002 (FISMA), the Farm Credit Administration's (FCA or Agency) Chief Information Officer (CIO) and Inspector General (IG) are responsible for conducting annual assessments of the Agency's information security program and reporting the results to the Office of Management and Budget (OMB). Under contract with the FCA's Office of Inspector General (OIG), Harper, Rains, Knight & Company, P.A. (HRK) 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 objectives, scope, methodology, and results of our evaluation of FCA's information security program. In addition, this report includes the IG reporting template (Appendix A) as required by OMB's FY 2007 Reporting Instructions for the FISMA in OMB Memorandum M-07-19.

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 CIO Council, and the National Institute of Standards and Technology (NIST).

We determined that FCA has an effective information security program. FCA conducted an annual self-assessment of the Agency's security program, categorized systems based on risk, applied a common security configuration, and completed certifications and accreditations on all Agency systems. In addition, FCA implemented an Agency-wide security awareness and training program, tested the Agency's continuity of operations plan, and followed a comprehensive incident response program.

We observed an active, engaged CIO with a cohesive, experienced, and well trained staff, which is proactive in their approach to information security and responsive to suggestions made during the FISMA evaluation. We also reviewed the CIO's plan to internally develop a Senior Agency Information Security Officer (SAISO) over the next fifteen months which includes requiring the SAISO to be a Certified Information Systems Security Professional (CISSP).

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

Objective

The objectives of the evaluation were to (1) assist the IG in responding to reporting requirements issued under OMB Memorandum M-07-19 and (2) verify and test the Agency's overall 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, 2007. 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, a contractor of an agency, or an 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. General Support Systems

    a. Microsoft Windows Operating System (Windows)

        Windows is an operating system, or the core program of a computer, that allows 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 Server is the primary operating system installed on servers in the FCA network. Additionally, Windows is 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, users can access network services such as file servers, e-mail, the Internet, applications and shared hardware such as printers.

2. Major Applications

    a. Lotus Domino (Notes)

        Lotus Domino (Notes) 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.

    b. Consolidated Reporting System (CRS)

        CRS is a 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:

- The 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. The 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.

- The LARS database contains specific loans of Farm Credit System lender institutions. Institutions electronically submit the data quarterly through FCA's secure Web site. The loan data is verified and validated by FCA personnel.

- The Web-based CRS Reports is an FCA developed application used for making reports 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 only available to authorized users.

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

   Oracle Federal Financials 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.

d. Personnel/Payroll System (PPS) from National Finance Center (NFC)

   NFC provides core personnel and payroll processing functions, including distributed application and telecommunications support for PPS, to FCA.

Methodology

HRK conducted this independent evaluation following the requirements found in GAO's Federal Information System Controls Audit Manual (FISCAM), OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," current NIST guidance, and the CIO Council Framework. We used these criteria to evaluate FCA's practices in determining compliance with FISMA.

Our evaluation was performed from April through September 2007 at FCA's headquarters in McLean, Virginia. This evaluation was performed in accordance with Government Auditing Standards, issued by the Comptroller General of the United States, for performance audits and applicable IS Auditing Standards, issued by the Information Systems Audit and Control Association (ISACA).

In performing this evaluation, we conducted interviews with key personnel, observed daily activities performed by FCA personnel, evaluated and reviewed policies and procedures provided by FCA, and evaluated the C&A and internal network security assessment (INSA) performed by external parties. HRK did not perform technical testing of FCA's information systems.

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 evaluations. We relied on the guidelines contained within NIST Special Publication 800-53A for evaluating information systems. Our assessment procedures included identifying the security controls for each system and determining whether those controls were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

NIST Special Publication 800-53A organizes security control assessment procedures into three "classes" of controls (management, operational, and technical). It further divides the three classes of controls into seventeen security control families. For each security control family, we 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. We exercised professional judgment in making such determinations. Below is a summary description of the seventeen security control families we assessed at FCA.

- **Management**
    - Risk assessment – Controls in place to categorize information systems in accordance with FIPS 199, assess the potential impact of unauthorized access, and 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 assessments – Controls in place to certify and accredit information systems and interconnected systems, perform continuous monitoring, and 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 protection – Controls in place for physical access to the building and information systems, visitor access, and preventative measures for physical damage to information systems components.
  - Contingency planning – Controls in place for planning, training, testing, and reviewing all contingency plans as well as providing alternative storage and processing sites.
  - Configuration management – Controls in place to document configuration information, monitor changes, and 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 response capability, detect incidents, and appropriately handle, monitor, and document incidents.
  - Awareness and training – Controls in place to implement security awareness and training for all employees including contractors, 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, authenticate devices on information system networks, and manage 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 identify auditable events, generate and review audit logs, and protect audit data and reports.
  - System and communications protection – Controls in place to separate user functionality from information system management functionality, protect against Internet attacks, and establish trusted communication paths between the user and the system.

The results were formally communicated to the CIO and responsible personnel from the Technology Team on September 13th. On September 17th we held a follow-up meeting with the CIO and key personnel from the Technology Team to discuss the OMB M-07-19 IG Reporting Template. We continued discussions via phone and email through September 25th, when we held an exit conference with the IG, the CIO, and their respective key personnel.

Results

Our procedures did not reveal any information system security control matters that we deemed to be significant deficiencies that must be reported under FISMA. Below you will find a summary of our observations from each of the security control families.

Risk assessment

FCA has controls in place to categorize information systems in accordance with FIPS 199, assess the potential impact of unauthorized access, and update the risk assessment, at least annually. FCA has policies and procedures in place and they are periodically reviewed. FCA categorizes information systems in accordance with FIPS 199. During fiscal year 2007, FCA lowered its FIPS 199 risk ranking from high to moderate for the general support system and CRS. We concur with these risk rankings. FCA conducts annual risk assessments of their information systems. FCA has a Continuity of Operations Plan (COOP) in place and it is reviewed annually. FCA has a system in place to track general security notifications and assess potential impact. While FCA has an Information Security Officer (ISO) that performs daily information security activities, the CIO has been acting as the SAISO. FCA has developed a plan that requires the ISO to obtain certification as a CISSP and take appropriate security training over the next fifteen months before being considered for the SAISO position.

Planning

FCA has controls to ensure a security plan is in place and to ensure the plan is readily available, updated regularly, and tested. FCA has policies and procedures in place and they are periodically reviewed. FCA has incorporated its security plans into the COOP plan. The security plans are reviewed annually and revised when appropriate. FCA provides training to employees on the expectations of using their information systems. 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, use a system development life cycle, and implement the information system using security engineering principles, where applicable. FCA has policies and procedures in place and they are periodically reviewed. The Information Resources Management (IRM) plan outlines and budgets for future information technology needs. FCA applies a system development life cycle to their information systems, and security is considered during FCA's information system planning and acquisition process. FCA tracks licenses and installations to comply with software usage restrictions. FCA does not allow software to be downloaded and installed unless it is supplied by FCA or approved on an individual basis. FCA designs and implements information systems using security engineering principles.

Certification, accreditation, and security assessments

FCA has controls in place to certify and accredit information systems and interconnected systems, perform continuous monitoring, and develop and update the POA&M. FCA has policies and procedures in place and they are periodically reviewed. 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. FCA authorizes all interconnections to other information systems outside the accreditation boundary and monitors/controls the information system interconnections on an ongoing basis. FCA has a process to develop, update, and report POA&Ms as required by OMB. FCA has a policy and performs C&As on its information systems every three years or when significant information system changes occur. FCA plans to require the system owners to sign-off on the C&A and authorization to operate (ATO) documents beginning in FY 2008.

Personnel Security

FCA has controls in place for employee screening, handling of terminated employees, and compliance failure sanctions. FCA has policies and procedures in place and they are periodically reviewed. Each FCA Position Description (PD) has a "Position Sensitivity" indicator. FCA employees are not granted access to information systems without a sponsor's approval. When an employee is terminated, quits, or retires, FCA requires the individual to complete a separation checklist. 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 policy.

Physical and environmental protection

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

The Technology Team offices are located on a high traffic common floor with non-FCA tenants and the building's cafeteria. We observed the side-entrance doors to the offices were closed and locked. We found the door at the main entrance to the offices was open during work hours. However, we noted all entrance doors were clearly marked "FCA Personnel Only." We observed the nightly cleaning crew unlock and open all doors in the offices when on-site. The guards periodically check and secure the doors after the cleaning crew has left the premises. The CIO has plans to use the Fairfax County Police Department to assist FCA with addressing the

concerns identified with the nightly cleaning crew and appropriately securing doors to sensitive FCA office space as well as other physical security issues.

Contingency planning

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

Configuration management

FCA has controls in place to document configuration information, monitor changes, and restrict access to information systems. FCA has policies and procedures in place and they are periodically reviewed. Information system changes are tested and monitored after being placed in production. FCA has established configuration settings for information technology, set default access as none, and enforces configuration settings in all components of the information system. FCA has adopted a standard configuration policy that incorporates the intent of the NIST baseline security configurations. In addition, FCA plans to adopt the NIST baseline security configurations with all new technology implemented as well as document any deviations from the NIST security configurations on all systems.

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. FCA has policies and procedures in place and they are periodically reviewed. FCA runs Hewlett Packard (HP)/Compaq Insight System Manager, which monitors the health of servers and reports on problems via email. FCA controls and monitors maintenance on FCA laptops. 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. FCA has policies and procedures in place and they are periodically reviewed. FCA has virus protection software installed and it updates automatically. FCA continuously monitors the information systems to detect attacks and prevent unauthorized use. FCA participates in the United States Computer Emergency Readiness Team (US-CERT) program. FCA restricts which personnel can make changes to the information systems. 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, appropriately mark and store media, and sanitize media when it is no longer needed. FCA has policies and procedures in place and they are periodically reviewed. FCA restricts user access to drives and applications. FCA labels do not indicate what is stored on the media and back up tapes are stored in a safe. However, we found system media is bar coded so that appropriate personnel can identify what is contained on each tape. 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 incident response roles, test their response capability, and actively monitor, respond, and document incidents. FCA periodically reviews and updates policies and procedures. FCA trains their employees to respond to incidents. FCA continually monitors for intrusions and documents and investigates unusual activity. We found during the current year FCA significantly enhanced their incident response handling capabilities.

Awareness and training

FCA has controls in place to implement security awareness and training for all employees including contractors, monitor training, and stay up to date with current technology and security practices. FCA has policies and procedures in place and they are periodically reviewed. FCA requires all employees complete an annual information technology security awareness training, and FCA performs additional security awareness activities through FCA newsletter and News Flash emails.

Identification and authentication

FCA has controls in place to identify and authenticate users of information systems, authenticate devices on information system networks, and manage users of information systems. FCA has policies and procedures in place and they are periodically reviewed. FCA users must be authenticated before accessing any resource. The encryption used on the Web site to access FCA information, Secure Socket Layer (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. FCA has policies and procedures in place and they are periodically reviewed. FCA deactivates accounts after a defined period of inactivity and passwords must be changed periodically. FCA uses least privilege access. FCA enforces segregation of duties through assigned authorization. FCA locks computers after three consecutive unsuccessful login attempts. FCA does not permit employees to use personally owned equipment to access the FCA network. Although FCA does not continuously monitor

those with administrative privileges to FCA's information systems, FCA has compensating controls that mitigate risks to systems.

Audit and accountability

FCA has controls in place to identify auditable events and generate, review, and protect audit data and reports. FCA has policies and procedures in place and they are periodically reviewed. FCA information systems generate and store logs which provide an audit trail. FCA is notified via email of suspicious events in addition to the event being recorded in the log. FCA has the ability to produce audit trail reports from the firewall and intrusion detection system. FCA's event/audit logs include time stamps. 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 information systems management functionality, protect against Internet attacks, and establish trusted communication paths between the user and the system. FCA has policies and procedures in place and they are periodically reviewed. FCA separates information system user functionality from information system management functionality. FCA has controls in place to limit the effects of common attacks, including denial of service attacks. FCA has controls in place to ensure high priority processes, such as virus scans, have access to needed resources. FCA information is transmitted by secure means such as SSL when appropriate. FCA terminates remote connections after 30 minutes of inactivity. FCA separates FOIA information from private information on the Web site.

APPENDIX A

OMB FISMA Reporting Template

Section C - Inspector General: Questions 1 and 2

Agency Name: **Farm Credit Administration** **Submission date:** **1-Oct-07**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Farm Credit Administration	High					0	0						
	Moderate	3	3	2	2	5	5	5	100%	5	100%	5	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**3**	**3**	**2**	**2**	**5**	**5**	**5**	100%	**5**	100%	**5**	100%
N/A	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
N/A	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
N/A	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
N/A	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
N/A	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Moderate	**3**	**3**	**2**	**2**	**5**	**5**	**5**	100%	**5**	100%	**5**	100%
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**3**	**3**	**2**	**2**	**5**	**5**	**5**	100%	**5**	100%	**5**	100%

Section C - Inspector General: Question 3		
Agency Name:	**Farm Credit Administration**	
	Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of 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.** 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. 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 (96-100% of the time)
3.b.	**The agency has developed a complete 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: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG 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 or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes
3.f.	**If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**	

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI)	Agency or Contractor system?

Section C - Inspector General: Questions 4 and 5

Agency Name: Farm Credit Administration

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

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**

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 (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 (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Almost Always (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 (96-100% of the time)

FCA does not have any outstanding POA&M items as of September 14, 2007.

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

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, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good	
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	

C&A process comments: FCA has completed its first three-year cycle for the C&A process, including completing C&As on all agency systems, however, this process is in its infancy and must become an established, reoccurring process within the agency.

Section C - Inspector General: Questions 6 and 7		
Agency Name:		
Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	
	Comments: FCA has a process in place, which includes the involvement of the Office of General Council and the SAOP, to determine if a PIA is necessary. To date FCA has not been required to complete a PIA.	
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	**Excellent**
	Comments: Excluding FCA Employee Data, FCA does not store PII on FCA systems of record. FCA has policies and procedures in place to reduce risk when FCA examiners obtain PII ad hoc.	
Question 7: Configuration Management		
7.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
	Comments: FCA has adopted a standard configuration policy that incorporates the intent of the NIST baseline security configurations. FCA has plans to adopt the NIST baseline security configurations with all new technology implemented and document any deviations from the NIST security configurations on all systems.	
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **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 (96-100% of the time)

Section C - Inspector General: Questions 8, 9, 10 and 11		
Agency Name:		
Question 8: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes
	Comments:	
Question 9: Security Awareness Training		
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? **Response Categories:** **- Rarely- or approximately 0-50% of employees** **- Sometimes- or approximately 51-70% of employees** **- Frequently- or approximately 71-80% of employees** **- Mostly- or approximately 81-95% of employees** **- Almost Always- or approximately 96-100% of employees**		Almost Always (96-100% of employees)
Question 10: Peer-to-Peer File Sharing		
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**
Question 11: E-Authentication Risk Assessments		
The agency has completed system e-authentication risk assessments. Yes or No.		**Yes**

APPENDIX B

Acronyms and Abbreviations

ATO	Authorization to Operate
BPD	Bureau of Public Debt
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
COGCON	Continuity of Government Condition
COOP	Continuity of Operations Plan
CRS	Consolidated Reporting System
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
HRK	Harper, Rains, Knight & Company, P.A.
HP	Hewlett Packard
HVAC	Heating Ventilating and Air Conditioning
IG	Inspector General
INSA	Internal Network Security Assessment
IRM	Information Resource Management
ISO	Information Security Officer
LARS	Loan Account Reporting System
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
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 Milestones
PPS	Personnel/Payroll System
SAISO	Senior Agency Information Security Officer
SSL	Secure Socket Layer
System	Farm Credit System
US-CERT	United States Computer Emergency Readiness Team
Windows	Microsoft Windows Operating System