OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2009 Evaluation of the
Farm Credit Administration's
Compliance with the
Federal Information Security
Management Act

November 18, 2009

E-09-01

Tammy Rapp
Auditor-in-Charge

FARM CREDIT ADMINISTRATION

Memorandum

Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

November 18, 2009

The Honorable Leland A. Strom
Chairman of the Board
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Chairman Strom:

The Office of the Inspector General completed the 2009 independent evaluation of the Farm Credit Administration's compliance with the Federal Information Security Management Act (FISMA). The objectives of this evaluation were to perform an independent assessment of FCA's information security program and assess FCA's compliance with FISMA.

The results of our evaluation revealed that FCA has an effective information security program that complies with FISMA and did not identify any significant deficiencies in the Agency's information security program.

We appreciate the courtesies and professionalism extended to the evaluation staff. If you have any questions about this evaluation, I would be pleased to meet with you at your convenience.

Respectfully,

Carl A. Clinefelter
Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA) requires the Chief Information Officer (CIO) and Office of Inspector General (OIG) to conduct annual assessments of an agency's information security program and report the results to the Office of Management & Budget (OMB). This report contains the objectives, scope, methodology, and results of the OIG's evaluation of the Farm Credit Administration's (FCA or Agency) information security program. In addition, Appendix A contains the Inspector General (IG) Section Report as required by OMB's FY 2009 Reporting Instructions for the FISMA in OMB Memorandum M-09-29.

The results of our evaluation revealed that FCA has an effective information security program that continues to mature. FCA adopted a risk based approach to information security and implements new controls where weaknesses are identified that strengthen security while not becoming too burdensome. Some of the elements of the Agency's information security program include categorizing systems based on risk, developing security plans, implementing risk based security controls, applying a common security configuration, performing continuous monitoring, conducting a comprehensive security awareness program, testing the continuity of operations plan, and implementing an incident response program.

FCA has an engaged CIO with an information technology (IT) team that is experienced and well trained. The CIO and IT team are proactive in their approach to information security. The IT team was very responsive to minor suggestions made for improvement during the FISMA evaluation, and in many cases, the IT staff made immediate changes to strengthen the information security program where possible. The IT Security Specialist continues to work on her individual development plan to become a Certified Information Systems Security Professional (CISSP).

Our evaluation did not reveal any significant deficiencies in FCA's information security program and this report does not contain any recommendations or agreed-upon actions.

INTRODUCTION AND BACKGROUND

The President signed into law the E-Government Act (Public Law 107-347), which includes Title III, Information Security, on December 17, 2002. FISMA permanently reauthorized the Government Information Security Reform Act of 2000 which expired in November 2002. The purpose of FISMA was to strengthen the security of the Federal government's information systems and develop minimum standards for agency systems.

Section 3545 of FISMA requires OIGs to perform an annual independent evaluation of their agency's information security program to determine the effectiveness of the security program and practices. "Each evaluation under this section shall include—

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

(B) an assessment (made on the basis of the results of the testing) of compliance with—

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines;**"**

OMB issued Memorandum M-09-29, FY 2009 Reporting Instructions for the FISMA and Agency Privacy Management, on August 20, 2009. This memorandum provides instructions for complying with FISMA's annual reporting requirements and reporting on the agency's privacy management program. The most significant change to this year's reporting instruction from OMB was the method of data collection from agencies. OMB developed an automated reporting tool, CyberScope, which will be used by agencies in lieu of spreadsheet templates used in prior years.

OBJECTIVES

The objectives of this evaluation were to perform an independent assessment of FCA's information security program and assess FCA's compliance with FISMA.

SCOPE AND METHODOLOGY

The scope of this evaluation covered FCA's Agency-owned and contractor operated information systems of record as of September 30, 2009. FCA is a single program Agency with six mission critical systems: Infrastructure, Lotus Notes (Notes), Consolidated Reporting System (CRS), Personnel/Payroll System (PPS), Agency Financial Management System (AFMS), and electronic Official Personnel Folder system (eOPF).

Our evaluation included determination of the critical elements that are essential for establishing compliance with FISMA. Key criteria used to evaluate FCA's information security program and

compliance with FISMA included OMB guidance, National Institute of Standards and Technology (NIST) Special Publications (SP), and Federal Information Processing Standards Publications (FIPS). In performing this evaluation, we performed the following steps:

- Identified and reviewed Agency policies and procedures related to information security;
- Examined documentation relating to the Agency's information security program and compared to NIST standards and FCA policy;
- Conducted interviews with the CIO and other key personnel;
- Observed security related activities performed by Agency personnel; and
- Performed tests for a subset of controls.

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 SP 800-53A for evaluating information systems. Our assessment procedures included identifying the security controls for each system and determining whether a subset of those controls were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system. Since we completed an audit of the Agency's certification and accreditation (C&A) process in July 2009, we incorporated the results from that audit with this evaluation and built on our understanding from past FISMA evaluations. This evaluation represents the status of the information security program as of September 30, 2009, and did not include a test of all information security controls.

NIST SP 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 eighteen security control families. In addition to these security control families, we performed a limited evaluation of privacy issues in order to respond to OMB's reporting requirements for IGs. The conclusion section of this report summarizes our observations for each of these control families.

The evaluation's observations and results were presented to key IT personnel throughout the evaluation. On November 10, 2009, the CIO and OIG shared and discussed drafts of their respective FISMA section reports. On November 13, 2009, the OIG held an exit conference with the CIO and other key IT personnel to formally communicate the observations from this evaluation.

This evaluation was performed at the FCA headquarters in McLean, Virginia, from August 2009 through November 2009, in accordance with the former President's Council on Integrity and Efficiency's[1] *Quality Standards for Inspections*. This report is intended for use by FCA management and OMB.

[1] The PCIE was abolished by the Inspector General Reform Act of 2008 and replaced by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). CIGIE is now in the process of reviewing the Quality Standards for Inspections for any needed changes and will reissue them in the future under CIGIE's authorship.

CONCLUSIONS

Procedures performed during our evaluation did not reveal any significant deficiencies in FCA's information security program. Below you will find a summary of our observations from each of the security control families.

Information Security Program Management

FCA is committed to complying with the requirements of FISMA and improving its ability to protect personally identifiable information (PII). FCA's overall security program is integrated with the enterprise architecture (EA), capital planning and investment control process, and the life cycle management of each system. FCA's EA interacts with the capital planning and investment control process to ensure that IT investments support core business functions. FCA's EA also identifies security standards required for authentication and non-repudiation, audit trail creation and analysis, access controls, virus protection, and intrusion prevention and detection. FCA reviews and updates its information system inventory during the annual information resources management (IRM) planning and FISMA reporting cycles.

FCA developed policies that provide the foundation for an organization-wide information security program. FCA's security program is based on FISMA, OMB A-130, OMB security related memoranda, and NIST Special Publications and FIPS Publications. FCA is currently in the process of updating significant security policies and employee security certifications with its release of a new information system logon banner.

The CIO and the IT Security Specialist provide information security policy and assurance. Since FCA is a small agency, the CIO is responsible for many functions including the role of Senior Information Security Officer (or Chief Information Security Officer) and Senior Agency Official for Privacy. For the past few years, FCA has been transitioning the security related functions from the CIO to the IT Security Specialist, and the IT Security Specialist has been working towards obtaining the CISSP certification.

FCA has a process for developing plans of action and milestones (POA&M) for significant information security weaknesses and tracking their implementation. FCA's security philosophy is to correct identified deficiencies immediately, resulting in limited POA&M items. In addition, FCA uses its annual Management Control Plan to develop, monitor, and report on the performance and accountability of primary internal controls, including IT security. The results of the internal control reviews related to IT security indicated that most internal controls were validated as effective and operating as intended.

Risk Assessment

FCA performed periodic assessments of risk and potential harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations of the Agency. IT security and information protection needs were evaluated during the internal control reviews, capital investment planning and control process, and regular updates of the enterprise architecture, security plans, and other related security and IT policies. The security policy delegated responsibility to the CIO for periodically reviewing information systems to ascertain that security is proportionate to the risk.

Risk to information systems was continually assessed by evaluating security alerts, monitoring systems, and providing security related training. FCA maintained a vulnerability database, ran automated vulnerability detection tools, and reviewed the resulting lists of potential vulnerabilities. The security plan contained some elements of a risk assessment report as outlined in SP 800-30; however, it could be improved by describing threats and vulnerabilities, measuring the risk, and ensuring appropriate controls are identified and implemented.

The Agency added a new system during 2009. This system was categorized and the supporting rationale was documented in accordance with guidance from NIST.

Planning

FCA developed and implemented security plans that described the security controls for the general support system and major applications. Guidance from NIST was used to develop security plans. All security plans were updated during the past year, and a security plan was developed for a new system. FCA continues to improve its security plans and is in the process of revising its infrastructure security plan to identify the review cycle for each control as part of its continuous monitoring program. In addition, FCA plans to strengthen security plans over the next year by expanding the descriptions of controls implemented and ensuring consistency among the security plans. The IT Infrastructure security plan was updated on a regular basis throughout the year and not limited to the annual review cycle.

System and Services Acquisition

FCA implemented the following system and service acquisition controls. Specifically, the Agency has:

- Integrated security in the enterprise architecture, capital planning and investment control, and budgeting processes;
- Allocated sufficient resources to monitor and protect organizational information systems;

- Employed system development life cycle processes that incorporate information security considerations;
- Performed due diligence reviews and monitored security controls for outsourced systems; and
- Employed software usage and installation restrictions.

FCA ensured that its financial systems provider employed adequate security measures to protect information, applications, and services by performing site visits to review security documentation, performing data validations, and periodically reviewing user accounts and privileges. FCA strengthened its oversight of its payroll and personnel system provider by reviewing independent security assessments performed on the system and reviewing account lists to ensure access to Agency data was limited to authorized users. FCA plans to further strengthen oversight in 2010 by adding more specific controls to its security plans and performing site visits to review security related documentation for two outsourced systems.

Certification, Accreditation, and Security Assessments

FCA authorized information systems and connections, periodically assessed information security controls to determine their effectiveness, monitored security controls on an ongoing basis to ensure the continued effectiveness of the controls, and developed plans of corrective action to correct deficiencies and vulnerabilities.

The Agency's policy states the general support system and major applications will operate with proper accreditation and be recertified every 3 years or when a major system change occurs. All of FCA's systems have been certified and accredited, and all connections to FCA systems have been documented and authorized.

Recently, the OIG performed an audit of the FCA's C&A process used on its IT infrastructure during 2008. The results of our audit revealed that FCA's C&A process was well planned and managed, and complied with the requirements and guidance provided by the FISMA, OMB, and NIST. Our observations of the C&A process followed by the Agency disclosed the process contained the following elements:

- Proper and adequate planning;
- Security control testing executed in accordance with NIST guidance;
- No material gaps identified in security control testing;
- Appropriate reuse of previous assessments and evaluations;
- Adequate certification testing documentation;
- Accreditation decision based on balancing mission and operations with security; and
- Effective continuous monitoring program.

Periodic security assessments of the Agency's information systems are performed using a combination of continuous monitoring, self-assessments, and independent contractors. Issues identified during security assessments were resolved in a timely manner.

Continuous monitoring of security controls includes network security testing, configuration management, security event monitoring, security alert and vulnerability analysis, patch management, and intrusion detection monitoring. FCA has a process for developing plans of corrective action for significant information security weaknesses and tracking their implementation.

Personnel Security

The Agency's personnel security program includes classifying positions for sensitivity level and obtaining appropriate clearances for employees and contractors. FCA's Office of Management Services (OMS) identified personnel security as a control element in its Management Control Plan and tested related controls in 2009 to ensure appropriate records for background verifications and security clearances were established for FCA's personnel security related actions. When an employee terminates from the Agency, a separation checklist is completed.

Before providing system access, new employees and contractors are required to certify their understanding of FCA security policies and procedures. However, this policy does not apply to employees and contractors hired before 2000, and security certifications are not periodically updated even though security policies and procedures may have changed. FCA is in the process of revising its logon banner and significant information security policies. Once the policies are approved, all employees and contractors will be required to certify their understanding of applicable security policies.

In response to an issue identified during the 2008 FISMA evaluation, OMS improved its process for tracking contractors. The Personnel Security Officer and IT Security Specialist are notified prior to hiring a contractor so that adequate documentation and clearances are completed before providing the contractor with access to an information system.

Physical and Environmental Protection

FCA implemented several physical and environmental controls to limit physical access to the building and its information systems, monitor visitor access, and prevent physical damage to information system components. Physical and environmental protection was provided at FCA through the Farm Credit System Building Association (FCSBA). The FCSBA provides 24-hour guard protection, visitor access controls, and card readers for

entry into the building and sensitive areas. OMS performed quarterly reviews of physical access control lists to ensure access to the building and sensitive areas were limited to authorized individuals. Fire protection is provided by a halon system in the computer facility and sprinkler systems in the remainder of the building. The FCSBA performs regular maintenance on the heating and air conditioning systems and maintains an emergency backup generator. In addition, the computer facility has an uninterruptible power supply and redundant heating, ventilation, and air conditioning units. A specialized cleaning crew is used to maintain the environment in the computer facility.

Contingency Planning

FCA committed resources to ensure the continuity of operations of essential functions in emergency situations. A business continuity plan and disaster recovery plan were developed and periodically updated to support the restoration of operations and systems after a disruption or failure. In addition, FCA took precautionary measures with respect to the H1N1 flu including additional building cleaning, disseminating current information regarding the flu, providing seasonal flu vaccines to employees, and coordinating H1N1 vaccines for employees.

The Agency has an alternative IT processing site that was successfully activated during a government wide test. Employees from several offices participated in the test ensuring the availability of critical systems and alternative communication systems. Several managers and senior executives participated, including the Chairman of the Agency. The business continuity exercise generated productive discussions between functional areas regarding the importance of continuity planning, succession planning, communication, and prioritization of services. The exercise identified areas that need further testing or refinement, but no significant weaknesses were identified.

The Agency has an IT backup strategy that includes daily and weekly backups of data and systems. A disaster recovery kit is also maintained offsite that contains critical software needed to recreate systems. FCA has two off-site storage facilities for backups.

Configuration Management

FCA maintains a baseline configuration and enforces the security configuration settings for its information systems. Configuration management policies and procedures were developed and periodically updated. A standard configuration was maintained for laptops and servers. Any deviations to the standard configuration must be approved by the CIO. Both policy and technical settings prohibit most users from changing the configuration. An inventory of hardware and software components was maintained and updated regularly. FCA performed vulnerability assessments to confirm functions, ports, protocols, and services were limited to essential functions and services necessary to support operations.

To improve security of Federal information systems, OMB required agencies to adopt commonly accepted security configurations. In June 2008, NIST released the first major version of the Federal Desktop Core Configuration (FDCC)[2], which provided standard security settings for Windows XP and Vista. FCA successfully deployed some of the FDCC settings and is in the process of testing and implementing additional settings. Where deviations from the FDCC are necessary, justifications are developed and approved by the CIO. Because of the intense analysis and testing required to deploy over 400 FDCC settings, the Agency developed a POA&M.

Maintenance

FCA has an information system maintenance program with established controls over the tools, techniques, and personnel used to conduct information system maintenance. Most maintenance is performed by the Technology Team's (TT) staff on weekends to minimize disruption of IT services. When contractors are used to perform maintenance, they are closely supervised by TT personnel. Remote contractor access for diagnostic purposes is tightly controlled by IT staff. FCA maintains a current list of various maintenance and support agreements.

System and Information Integrity

FCA identifies and corrects information system flaws, monitors information system security alerts, maintains current patches on information systems, and provides protection from malicious code within information systems. Key IT personnel receive risk alerts from vendors and security organizations identifying information system flaws. These alerts are analyzed to determine the potential impact on Agency systems, tracked in a database, and remediated where applicable. In addition, key IT personnel participate in various list serves and security organizations that share information regarding new threats, vulnerabilities, and security practices. Anti-virus and anti-spam protection are installed on the Agency's information systems and updated automatically. E-mail messages and data files are scanned automatically without user intervention. FCA policy restricts employees from using USB thumb drives not issued by FCA on Agency laptops. If a thumb drive is received from other sources and needed for an FCA business purpose, it must be scanned by the Helpline to ensure they do not contain malicious software.

IT personnel continuously monitor audit logs, firewall logs, and security alerts. Controls implemented to ensure data integrity includes data entry validation, transaction log and error log review.

[2] The FDCC was developed by the NIST, the Department of Defense, and the Department of Homeland Security.

Media Protection

FCA issued policies and procedures and implemented several controls designed to protect sensitive information, including PII, on information system media. Sensitive information maintained on a local machine is protected by an encrypted hard drive. Employees that need to share sensitive data are provided with an encrypted USB drive and a local printer. The encrypted USB drives contain a feature that formats the data after several failed password attempts. Sensitive information in paper format is maintained in locked cabinets. The ability to create a CD or DVD has been disabled on the standard configuration, and the TT monitors USB ports for unauthorized devices.

FCA has documented procedures for protecting backup media. Access to backup media is limited to authorized personnel, stored in locked facilities, and transported in locked containers. Before disposal, backup media is sanitized preventing retrieval of the data.

Incident Response

FCA established an incident handling program that includes detection, reporting, analysis, containment, recovery, and user response activities. FCA has distributed several incident response policies and procedures over the past few years. In addition, staff was educated on the importance of reporting incidents to the Agency's Helpline of any IT equipment, PII, or sensitive data suspected to be missing, lost, or stolen. OMS maintains a 24 hour Helpline for reporting security incidents and provided employees with wallet cards with the contact information. A log is maintained of security incidents, and appropriate officials, including the OIG, are notified depending on the nature of the incident.

During the past year, OMS enhanced its information security program by identifying areas of improvement and implementing lessons learned from actual incidents. For example, there were several instances where employees failed to notify the Helpline within one hour of a security incident. As a result, OMS sent notices to all staff defining a security incident and reminding them of the importance of reporting any incidents immediately to the Helpline. Once incidents were reported to the Helpline, actions taken by OMS were timely and appropriate. OMS also implemented new procedures designed to mitigate potential infection from privileged network accounts in response to a Trojan that was identified on an Agency issued laptop.

Awareness and Training

FCA ensures users are aware of security risks associated with their activities by providing an ongoing IT security awareness program which includes formal training and e-mail alerts. New employees and contractors are provided with security awareness and privacy training before they are granted system access. In 2009, the IT Security

Specialist performed annual security awareness training for employees and contractors using small group sessions. The security awareness training focused on how to minimize risks from malicious software and the importance of reporting incidents immediately. Agency staff were periodically sent e-mails and news alerts that contain security tips and notices of new threats.

All employees and contractors with login privileges were provided with security awareness training during the past year. In addition, all IT specialists with significant information security responsibilities were provided with specialized training related to technology implemented at FCA during the past year.

Identification and Authentication

FCA identifies and authenticates information system users, processes, and devices before allowing access to information systems. Policies and procedures have been developed that support identification and authentication controls. In addition, OMS performed a risk assessment for e-authentication. Information system users are uniquely identified and authenticated on Agency information systems, and unauthorized devices are prevented from connecting to the Agency's network. Passwords are not displayed when entered and protected by encryption.

Access Control

FCA limits and monitors access to information systems to protect against unauthorized modification, loss, and disclosure. Policies and procedures for requesting, issuing, and closing information system accounts are documented. Information system accounts are created, managed, monitored, and disabled by authorized personnel. OMS controls access to information system data through groups and permissions assigned to files, folders, and databases. Users of FCA information systems are provided with the least amount of system access needed to perform their responsibilities, and sensitive database access is granted only after authorization from an employee's supervisor and the system sponsor. During 2009, TT strengthened security for privileged network access. Periodically, information system sponsors review accounts to ensure access permissions provided to information system users is current and appropriate. OMS uses a combination of technical configuration settings and other automated controls to prevent, detect, or notify authorized individuals of suspicious account activity. Remote access to FCA's information systems is controlled through a virtual private network (VPN). FCA intends to expand the use of HSPD12 cards for logical access to computers and networks with the next generation of laptops.

Audit and Accountability

FCA creates, protects, and retains audit records for its information systems. Policies and procedures were established to identify events which FCA determined as significant and

relevant to the security of the information system. Access to audit logs is restricted to authorized individuals. Administrators are automatically notified by e-mail of suspicious events and audit processing failures, and the CIO is notified of significant events. Unusual activity is investigated and necessary action is taken by appropriate personnel. Audit events are recorded in an audit log which is periodically archived.

System and Communications Protection

FCA has established controls that separate user functionality from information system management functionality, protect against external attacks, and establish trusted communication paths between the user and the system. System communications at key boundaries and interfaces are monitored and controlled. Internal networks are protected at all connection points to the internet. A VPN provides for secure encrypted transmission of data outside of the Agency's network. Encryption is used to protect sensitive data and PII.

Privacy Related

Our review of privacy matters was limited to obtaining sufficient information to respond to the privacy related questions in OMB's template for IGs. FCA does not have any systems that collect PII regarding members of the public, and therefore has not conducted any privacy impact assessments. In response to various OMB memorandums, the Agency reviewed the use of social security numbers and the collection of PII and other sensitive information throughout the Agency. FCA reduced the collection of sensitive information to the minimum necessary to perform Agency functions. The Agency also implemented safeguards such as encryption and employee training to protect sensitive data. In 2009, the Agency developed two official confidentiality notices that may be attached to e-mail messages related to sensitive supervision or examination activities and other types of business communications.

Inspector General

Section Report

2009

Annual FISMA Report

Farm Credit Administration

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

1. Identify the number of Agency and contractor systems by component and FIPS 199 impact level (low, moderate, high) reviewed.

2. For the Total Number of Reviewed Systems Identified 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
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
FCA	High	0	0	0	0	0	0	0	0	0
	Moderate	3	3	3	3	6	6	6	6	6
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	3	3	3	3	6	6	6	6	6
Agency Totals	High	0	0	0	0	0	0	0	0	0
	Moderate	3	3	3	3	6	6	6	6	6
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Total Systems	3	3	3	3	6	6	6	6	6

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

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.

3a. Does the Agency have policies for oversight of contractors?

No

Comments:

Although FCA does not have documented policies addressing oversight of contractor systems, FCA performed due diligence of its contractor systems. FCA reviewed independent security assessments, obtained signed interconnection agreements, and performed site visits of its financial systems provider to review security documentation.

In addition, FCA developed security plans for each contractor system, performed data validations, and periodically reviewed user accounts and privileges.

3b. Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency?

Yes

3c. Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency?

Yes

3d. Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency?

Yes

Comments:

The Agency has agreements for all system interconnections.

3e. The Agency inventory is maintained and updated at least annually.

Yes

3f. The IG generally agrees with the CIO on the number of Agency-owned systems.

Yes

3g. 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

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, providing explanatory detail in the area provided.

4a. Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?

Yes

4a(1). Has the Agency fully implemented the policy?

Yes

4b. Is the Agency currently managing and operating a POA&M process?

Yes

4c. Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weakness, including IG/external audit findings 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?

Yes

4d. Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?

Yes

4e. When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?

Yes

4f. For Systems Reviewed:

4f(1). Are deficiencies tracked and remediated in a timely manner?

Yes

4f(2). Are the remediation plans effective for correcting the security weakness?

Yes

4f(3). Are the estimated dates for remediation reasonable and adhered to?

Yes

4g. Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?

Yes

4h. Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?

Yes

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the Agency's certification and accreditation (C&A) 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" for C&A work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

5a. Has the Agency developed and documented an adequate policy for establishing a C&A process that follows the NIST framework?

Yes

5b. Is the Agency currently managing and operating a C&A process in compliance with its policies?

Yes

5c. For Systems reviewed, does the C&A process adequately provide:

5c(1). Appropriate risk categories

Yes

5c(2). Adequate risk assessments

Yes

5c(3). Selection of appropriate controls

Yes

5c(4). Adequate testing of controls

Yes

5c(5). Regular monitoring of system risks and the adequacy of controls

Yes

5d. For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented?

Yes

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

Provide a qualitative assessment of the Agency's process, as discussed in the SAOP section, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.

6a. Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?

Yes

6b. Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?

Yes

6c. Has the Agency developed and documented an adequate policy for PIAs?

Yes

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

6d. Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate PIAs?

Yes

Comments: FCA does not have any systems that collect PII regarding members of the public, and therefore has not conducted any privacy impact assessments.

Question 7: Configuration Management

7a. Is there an Agency wide security configuration policy?

Yes

7a(1). For each OS/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy.

OS/Platform/System	Implementation Status
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: [redacted] — Tool Category: [redacted]

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

OS/Platform/System	Implementation Status
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** **Tool/Technique Name** / **Tool Category** [redacted] / [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** **Tool/Technique Name** / **Tool Category** [redacted] / [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** **Tool/Technique Name** / **Tool Category** [redacted] / [redacted] [redacted] / [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** **Tool/Technique Name** / **Tool Category** [redacted] / [redacted] [redacted] / [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** **Tool/Technique Name** / **Tool Category** [redacted] / [redacted] [redacted] / [redacted]

<table>
<tr><th>OS/Platform/System</th><th>Implementation Status</th></tr>
<tr><td>[redacted]</td><td>[redacted]
What tools and techniques is your Agency using for monitoring compliance?
<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>[redacted]</td><td>[redacted]</td></tr><tr><td>[redacted]</td><td>[redacted]</td></tr></table></td></tr>
<tr><td>[redacted]</td><td>[redacted]
What tools and techniques is your Agency using for monitoring compliance?
<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>[redacted]</td><td>[redacted]</td></tr><tr><td>[redacted]</td><td>[redacted]</td></tr></table></td></tr>
<tr><td>[redacted]</td><td>[redacted]
What tools and techniques is your Agency using for monitoring compliance?
<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>[redacted]</td><td>[redacted]</td></tr><tr><td>[redacted]</td><td>[redacted]</td></tr></table></td></tr>
<tr><td>[redacted]</td><td>[redacted]
What tools and techniques is your Agency using for monitoring compliance?
<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>[redacted]</td><td>[redacted]</td></tr><tr><td>[redacted]</td><td>[redacted]</td></tr></table></td></tr>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]
What tools and techniques is your Agency using for monitoring compliance?
<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>[redacted]</td><td>[redacted]</td></tr><tr><td>[redacted]</td><td>[redacted]</td></tr></table></td></tr>
</table>

OS/Platform/System	Implementation Status
[redacted]	[redacted] What tools and techniques is your Agency using for monitoring compliance? Tool/Technique Name: [redacted] — Tool Category: [redacted] Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] What tools and techniques is your Agency using for monitoring compliance? Tool/Technique Name: [redacted] — Tool Category: [redacted] Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] What tools and techniques is your Agency using for monitoring compliance? Tool/Technique Name: [redacted] — Tool Category: [redacted] Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] What tools and techniques is your Agency using for monitoring compliance? Tool/Technique Name: [redacted] — Tool Category: [redacted] Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] What tools and techniques is your Agency using for monitoring compliance? Tool/Technique Name: [redacted] — Tool Category: [redacted] Tool/Technique Name: [redacted] — Tool Category: [redacted]

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

OS/Platform/System	Implementation Status
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: [redacted] — Tool Category: [redacted]
[redacted]	[redacted] **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: [redacted] — Tool Category: [redacted]

Comments: Although the OIG did not perform independent verification of the CIO's response on each of the OS/platform/systems listed, we observed results from a recent [redacted] scan performed by IT personnel that did not reveal any high or medium vulnerabilities.

7b. Indicate the status of the implementation of Federal Desktop Core Configuration (FDCC) at your Agency:

7b(1). Agency has documented deviations from FDCC standard configuration.

No

Comments: FCA successfully deployed approximately 25% of the FDCC settings and in the process of testing additional settings. Where deviations from the FDCC are necessary, justifications are developed and approved by the CIO. The Agency developed a plan of action and milestones for the FDCC.

7b(2). New Federal Acquisition Regulation 2008-004 language, which modified "Part 39-Acquisition of Information Technology," is included in all contracts related to common security settings.

No

Comments: Although FCA is not required to follow the FAR, new acquisitions must comply with standard FCA security configurations.

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

Question 8: Incident Reporting

8a. How often does the Agency comply with documented policies and procedures for identifying and reporting incidents internally?

60 % to 70 %

Comments: There were several instances where employees failed to notify the Helpline within one hour of a security incident. Once incidents were reported to the Helpline, actions taken were timely and appropriate.

8b. How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US-CERT?

100 % to 100 %

Comments: Once the incident was reported internally to the Helpline, US-CERT was notified timely. Three incidents were reported to US-CERT during FY 2009.

8c. How often does the Agency follow documented policies and procedures for reporting to law enforcement?

100 % to 100 %

Comments: One incident was reported to law enforcement during FY 2009.

Question 9: Security Awareness Training

Provide an assessment of whether the Agency has provided IT security awareness training to all users with log-in privileges, including contractors. Also provide an assessment of whether the Agency has provided appropriate training to employees with significant IT security responsibilities.

9a. Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log-in privileges, and providing them with suitable IT security awareness training?

Yes

9b. Report the following for your Agency:

9b(1). Total number of people with log-in privileges to Agency systems.

290

Comments: Includes employees and contractors as of 9/16/2009.

APPENDIX A: INSPECTOR GENERAL SECTION REPORT for OMB

9b(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."

290 **(100 %)**

Comments: as of 11/6/2009

9b(3). Total number of employees with significant information security responsibilities.

29

9b(4). Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model."

29 **(100 %)**

Question 10: Peer-to-Peer File Sharing

10. Does the Agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other Agency-wide training?

Yes

APPENDIX B: ACRONYMS AND ABBREVIATIONS

AFMS	Agency Financial Management System
Agency	Farm Credit Administration
C&A	certification and accreditation
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
CRS	Consolidated Reporting System
EA	enterprise architecture
eOPF	electronic Official Personnel Folder system
FCA	Farm Credit Administration
FCSBA	Farm Credit System Building Association
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards Publications
FISMA	Federal Information Security Management Act
IG	Inspector General
IRM	information resources management
IT	information technology
NIST	National Institute of Standards and Technology
Notes	Lotus Notes
OIG	Farm Credit Administration's Office of Inspector General
OMB	Office of Management & Budget
OMS	Farm Credit Administration's Office of Management Services
PII	personally identifiable information
POA&M	plan of action and milestones
PPS	Personnel/Payroll System
SP	Special Publication
TT	Technology Team
VPN	virtual private network

R E P O R T

Fraud | Waste | Abuse | Mismanagement

FARM CREDIT ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

- Phone: Toll Free (800) 437-7322; (703) 883-4316
- Fax: (703) 883-4059
- E-mail: fca-ig-hotline@rcn.com
- Mail: Farm Credit Administration
  Office of Inspector General
  1501 Farm Credit Drive
  McLean, VA 22102-5090