

Office of Inspector General

OIG 2008 Evaluation of the
Farm Credit Administration's
Compliance with the
Federal Information Security
Management Act

E-08-01

Tammy Rapp
Auditor-in-Charge



September 29, 2008

Memorandum

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



September 29, 2008

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 (OIG) completed the 2008 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.

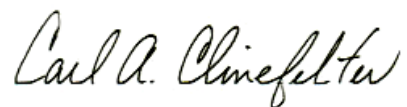
This evaluation was performed by our internal Senior Information Technology Auditor. In previous years, the OIG contracted with an independent public accounting firm to perform the evaluation and assist in reporting requirements to the Office of Management and Budget.

The results of our evaluation revealed that FCA has an effective information security program and did not identify any significant deficiencies in the Agency's information security program. We did note a few areas where improvement can be made, and the Office of Management Services (OMS) agreed to take action to strengthen the following areas of the Agency's information security program:

- Implement a policy review and revision cycle to ensure that information security policies and procedures are current and accommodate the information security environment and operational requirements.
- Update the security policies and security plans to reflect the frequency and types of security assessments to be performed. In addition, arrange for an independent third party to perform a penetration test of its infrastructure.
- Improve the process for information system access agreements by periodically requiring employees and contractors to recertify their understanding of FCA security policies and procedures. In addition, the Personnel Security Officer and IT Security Specialist should be notified prior to a contractor being hired so they can ensure that all appropriate documentation and clearances have been completed prior to providing information system access.

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,

A handwritten signature in cursive script that reads "Carl A. Clinefelter". The signature is written in black ink and is positioned above the typed name.

Carl A. Clinefelter
Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
INTRODUCTION AND BACKGROUND.....	2
OBJECTIVES.....	2
SCOPE AND METHODOLOGY.....	2
CONCLUSIONS AND AGREED-UPON ACTIONS.....	4
Information Security Governance.....	4
Risk Assessment	4
Planning	5
System and Services Acquisition.....	5
Certification, Accreditation, and Security Assessments.....	6
Personnel Security	6
Physical and Environmental Protection	7
Contingency Planning.....	7
Configuration Management.....	8
Maintenance	8
System and Information Integrity	9
Media Protection	9
Incident Response	9
Awareness and Training	9
Identification and Authentication.....	10
Access Control.....	10
Audit and Accountability.....	10
System and Communications Protection.....	10
Privacy Related	11
APPENDIX A: OMB REPORTING TEMPLATE FOR IGS.....	12
APPENDIX B: ACRONYMS AND ABBREVIATIONS	17

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, this report includes the IG reporting template (Appendix A) as required by OMB's FY 2008 Reporting Instructions for the FISMA in OMB Memorandum M-08-21.

The results of our evaluation revealed that FCA has an effective information security program. Some of the elements of the Agency's information security program include categorizing systems based on risk, developing security plans, 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 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) and complete the required examination by the end of 2008.

Although our evaluation did not reveal any significant deficiencies in FCA's information security program, we did note a few areas where improvement can be made. The OMS agreed to take action on the following areas which will strengthen the Agency's information security program:

- Implement a policy review and revision cycle to ensure that information security policies and procedures are current and accommodate the information security environment and operational requirements.
- Update the security policies and security plans to reflect the frequency and types of security assessments to be performed. In addition, arrange for an independent third party to perform a penetration test of its infrastructure.
- Improve the process for information system access agreements by periodically requiring employees and contractors to recertify their understanding of FCA security policies and procedures. In addition, the Personnel Security Officer and IT Security Specialist should be notified prior to a contractor being hired so they can ensure that all appropriate documentation and clearances have been completed prior to providing information system access.

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-08-21, FY 2008 Reporting Instructions for the FISMA and Agency Privacy Management, on July 14, 2008. This memorandum provides instructions for complying with FISMA's annual reporting requirements and reporting on the agency's privacy management program.

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 June 30, 2008. FCA is a single program Agency with five mission critical systems: Infrastructure, Lotus Notes, Consolidated Reporting System, Personnel/Payroll System, and Agency Financial Management System.

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 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. The emphasis of our evaluation was focused on items that changed since the prior FISMA evaluation.

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 seventeen security control families. In addition to these security control families, we evaluated information security governance and limited privacy issues.

The evaluation's observations and results were presented to key IT personnel throughout the evaluation. On September 18, 2008, the CIO and OIG shared and discussed their respective OMB templates. On September 23, 2008, the OIG held an exit conference with the CIO and other key IT personnel to formally communicate the observations and recommendations resulting from this evaluation.

This evaluation was performed at the FCA headquarters in McLean, Virginia, from June 2008 through September 2008, in accordance with the President's Council on Integrity and Efficiency's (PCIE) *Quality Standards for Inspections*.

CONCLUSIONS AND AGREED-UPON ACTIONS

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 Governance

FCA is committed to complying with the requirements of FISMA and improving its ability to protect personally identifiable information (PII). Information security management is integrated into the Agency's information resources management (IRM) planning process and enterprise architecture. The Agency's IRM Plan and enterprise architecture are reviewed and updated on an annual basis. The Information Resources Management Operations Committee (IRMOC) reviews IRM projects for alignment with FCA's enterprise architecture. In addition, proposed projects are analyzed for network demands and security risks.

Policies and procedures were developed that identify security controls, information security roles and responsibilities, and rules of behavior that users are expected to follow. FCA has updated and developed many new policies and procedures over the past two years; however, some of the information security policies are still outdated. For example, Policies and Procedures Manual (PPM) #902 does not refer to any of the provisions contained in FISMA but refers to the Computer Security Act which was superseded by FISMA.

The IT Security Specialist maintains a security folder accessible by all FCA staff in a centrally located database that contains Agency security policies, procedures, and guidance. This folder was well organized, easy to find, and intuitive.

Agreed-upon Action:

1. The OMS will implement an annual policy review and revision cycle of information security policies and procedures to ensure they are current and accommodate the information security environment and operational requirements. OMS will update policies and procedures as part of an ongoing process that addresses these areas as well as guidance from OMB, NIST, and the Department of Homeland Security (DHS).

Risk Assessment

FCA has controls in place to minimize the risk of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the

Agency. The security policy delegated responsibility to the CIO for periodically reviewing information systems to ascertain that security is proportionate to the risk. The Agency categorizes systems and documents the supporting rationale in accordance with FIPS 199. Risk to information systems is continually assessed by evaluating security alerts, monitoring systems, and providing security related training. FCA maintains a vulnerability database, runs automated vulnerability detection tools, and reviews the resulting lists of potential vulnerabilities. The security plan contains 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.

Planning

FCA developed and implemented security plans describing the security controls for all general support systems and major applications. Security plans are reviewed and updated annually.

An evaluation of the IT infrastructure security plan demonstrated that it was closely aligned with the requirements of SP 800-18. The IT infrastructure security plan provides an overview of the security requirements for the infrastructure, describes specific controls that are implemented, and delineates responsibilities for each control. The IT infrastructure security plan incorporates the minimum security requirements and controls identified in FIPS 200 and SP 800-53. It also refers to several related policies and procedures supporting individual controls. Minor editorial issues were identified and communicated to the IT Security Specialist and TT Team Leader.

System and Services Acquisition

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

- integrated security in the enterprise architecture, IRM planning, and budgeting processes;
- allocated sufficient resources to protect organizational information systems;
- employed system development life cycle processes that incorporate information security considerations; and
- employed software usage and installation restrictions.

FCA has ensured that its financial systems provider employs 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 is in the process of strengthening oversight of its payroll and personnel system provider by reviewing independent security assessments performed on the system and requesting account lists to ensure Agency data is limited to authorized users.

Certification, Accreditation, and Security Assessments

FCA authorizes information systems and connections, periodically assesses information security controls to determine their effectiveness, monitors security controls on an ongoing basis to ensure the continued effectiveness of the controls, and develops 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 the infrastructure is currently in the process of reaccreditation. All connections to FCA systems have been documented and authorized.

Periodic security assessments of the Agency's information systems are performed using a combination of self-assessments and independent contractors. Historically, OMS evaluates the current information security climate and determines the type of security assessment to be performed. However, the Agency's security policy and security plans do not define the frequency of security assessments performed internally or by an independent third party. FCA made major changes to its infrastructure during 2008 but has not arranged for a penetration test. A penetration test is generally performed by technical experts whose purpose is to simulate a malicious attack and evaluate the technical security controls of the system. The results of a penetration test are used to strengthen the security of the system and provide some assurance that the infrastructure's security controls will prevent most malicious attacks.

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

Agreed-upon Action:

2. OMS will update the infrastructure security plan to incorporate the annual process of conducting self assessments and arranging for independent security assessments. In addition, OMS will arrange for an independent third party to perform the annual penetration test of the infrastructure by June 2009.

Personnel Security

The Agency's personnel security program includes classifying positions for sensitivity level and obtaining appropriate clearances for employees and contractors. 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. When an employee terminates from the Agency, a separation checklist is completed.

When offices have staff shortages or require the expertise of an independent contractor, they sometimes use the services of a contractor or temporary employee. The Personnel Security Officer and IT Security Specialist are not always notified or notified late in the process before the contractor comes on board. The Personnel Security Officer and IT Security Specialist are responsible for ensuring contractors have appropriate background clearances and understand FCA's security policies.

Agreed-upon Action:

3. As OMS implements a regular policy and procedure review (see Information Security Governance), they will implement a process of requiring all employees and contractors to recertify their understanding of FCA security policies and procedures when updates to major security documents are made. In addition, the OMS will create a formal process that notifies the Personnel Security Officer and IT Security Specialist prior to a contractor being hired so that adequate documentation and clearances are complete before providing them with access to an information system.

Physical and Environmental Protection

FCA implemented 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 is provided at FCA through the Farm Credit System Building Association (FCSBA). The FCSBA provides 24-hour guard protection, visitor access controls, and key cards for entry into the building and sensitive areas. 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. Specialized cleaners are used to maintain the environment in the computer facility.

Contingency Planning

FCA has committed resources to ensure the continuity of operations of essential functions in emergency situations. A business continuity plan and disaster recovery plan were developed to support the restoration of operations and systems after a disruption or failure. The business continuity and disaster recovery plans are periodically updated. The Agency has an alternative processing site that was successfully activated during a government wide test in

2008. Employees from several offices participated in the test ensuring the availability of all critical systems. The Federal Emergency Management Agency (FEMA) evaluated FCA's performance during the test and concluded FCA "operated outstandingly." FEMA did note some areas that needed improvements and FCA is working with FEMA to improve its testing, training, and exercise program.

The Agency has a 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 are periodically updated. A standard configuration is 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 is maintained and updated regularly. FCA performs vulnerability assessments to confirm functions, ports, protocols, and services are limited to essential functions and services necessary to support operations.

To improve security of federal information systems, OMB requires agencies to adopt commonly accepted security configurations. In June 2008, NIST released the first major version of the Federal Desktop Core Configuration (FDCC)¹ which provides standard security settings for Windows XP and Vista. In addition, agencies are required to use FDCC scanning tools that validate compliance as part of their FISMA continuous monitoring. FCA has successfully deployed some of the FDCC settings and in the process of testing and implementing additional settings. Where deviations from the FDCC are necessary, a justification will be developed and approved by the CIO. Because of the intense analysis and testing required to deploy over 700 FDCC settings, the Agency developed a plan of action and milestones (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 FCA staff on weekends to minimize disruption of IT services. When contractors are used to perform maintenance, they are closely supervised by FCA personnel. FCA maintains a current list of various maintenance and support agreements. Remote contractor access for diagnostic purposes is tightly controlled by IT staff.

¹ The FDCC was developed by the NIST, the Department of Defense, and the DHS.

System and Information Integrity

FCA identifies and corrects information system flaws, monitors information system security alerts and takes appropriate actions in response, and provides protection from malicious code within information systems. FCA receives 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. Email messages and data files are scanned automatically without user intervention.

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.

Media Protection

FCA protects information system media by limiting access to information system media, and destroying information system before disposal. 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. Sensitive information in paper format is maintained in locked cabinets.

FCA has documented procedures for protecting backup tapes. Access to backup media is limited to authorized personnel, stored in locked facilities, and transported in locked containers. Backup media is sanitized before disposal.

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 two years. In addition, staff was educated on the importance of reporting incidents to the Agency's helpline within one hour of any IT equipment, personally identifiable information, or sensitive data suspected to be missing, lost, or stolen. A log is maintained of incidents, and appropriate officials, including the OIG, are notified.

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. In 2008, the IT Security Specialist performed security awareness training for

employees and contractors using small group question and answer sessions. In addition, users were reminded where security policies and procedures were maintained for further reference. Agency staff are periodically sent e-mails and news alerts that contain security tips and notices of new threats.

In the past year, all IT specialists were provided with specialized training related to new technology implemented at FCA.

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, FCA 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. FCA has plans to implement dual factor authentication during 2009.

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. Periodically, information system accounts are reviewed. Access to information system data is controlled through groups and permissions assigned to files, folders, and databases. Sensitive database access is granted only after authorization from an employee's supervisor and the system sponsor. After a predefined number of invalid login attempts, network accounts are locked. Remote access to information systems is controlled through a virtual private network.

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 administrators. Administrators are automatically notified by e-mail of suspicious events, and the CIO is notified of significant events. 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. Internal networks are protected at

all connection points to the internet. A virtual private network (VPN) provides for a secure encrypted transmission of data outside of the Agency's network. Encryption is used to protect sensitive data and personally identifiable information.

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.

APPENDIX A: OMB Reporting Template for IGs

Section C - Inspector General: Questions 1 and 2													
Agency Name: Farm Credit Administration							Submission date: September 30, 2008						
Question 1: FISMA Systems Inventory													
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>													
Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing													
<p>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.</p>													
Bureau Name	FIPS 199 System Impact Level	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	
		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
Component/Bureau	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%
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	0	0	0	0	0	0	0		0		0	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	0	0	0	0	0	0	0		0		0	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	0	0	0	0	0	0	0		0		0	
Component/Bureau	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: 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)

POA&M process comments:

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.	<p>The IG rates the overall quality of the Agency's certification and accreditation process as:</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Excellent - Good - Satisfactory - Poor - Failing 	Good																
5.b.	<p>The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)</p> <table border="1" style="width: 100%;"> <tr><td>Security plan</td><td style="text-align: center;">X</td></tr> <tr><td>System impact level</td><td style="text-align: center;">X</td></tr> <tr><td>System test and evaluation</td><td style="text-align: center;">X</td></tr> <tr><td>Security control testing</td><td style="text-align: center;">X</td></tr> <tr><td>Incident handling</td><td style="text-align: center;">X</td></tr> <tr><td>Security awareness training</td><td style="text-align: center;">X</td></tr> <tr><td>Configurations/patching</td><td style="text-align: center;">X</td></tr> <tr><td>Other:</td><td></td></tr> </table>	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:		
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:

Section C - Inspector General: Questions 6, 7, and 8		
Agency Name: Farm Credit Administration		
Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	<p>Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.</p> <p>Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing</p>	
Comments:	n/a - FCA does not have any systems that collect personally identifiable information (PII) regarding members of the public, and therefore has not conducted any privacy impact assessments.	
7	<p>Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.</p> <p>Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing</p>	Excellent
Comments:	FCA reviewed the use of social security numbers and the collection of PII and sensitive information throughout the agency. FCA has reduced the collection of sensitive information to the minimum necessary to perform agency functions. Although FCA does not collect PII regarding members of the public, it has implemented additional safeguards such as encryption and employee training.	
Question 8: Configuration Management		
8.a.	Is there an agency-wide security configuration policy? Yes or No.	Yes
Comments:	FCA has a standard configuration for agency laptops and servers. Any deviations from the standard configuration must be approved by the CIO. The configuration policy is enforced by preventing users from installing software and network monitoring. In addition, FCA is in the process of testing and implementing the FDCC standard configurations.	
8.b.	<p>Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.</p> <p>Response categories:</p> <ul style="list-style-type: none"> - 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 	Mostly (81-95% of the time)
8.c.	Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	No
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	No
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

Section C - Inspector General: Questions 9, 10 and 11	
Agency Name:	Farm Credit Administration
Question 9: 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.	
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No. Yes
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov) Yes
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No. Yes
Comments:	
Question 10: Security Awareness Training	
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?	Almost Always (96-100% of employees)
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	
Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing	
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	Yes
Question 12: E-Authentication Risk Assessments	
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.	Yes
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	

APPENDIX B: ACRONYMS AND ABBREVIATIONS

Agency	Farm Credit Administration
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
DHS	Department of Homeland Security
FCA	Farm Credit Administration
FCSBA	Farm Credit System Building Association
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards Publications
FISMA	Federal Information Security Management Act
IRM	information resources management
IRMOC	Information Resources Management Operations Committee
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Farm Credit Administration's Office of Inspector General
OMB	Office of Management & Budget
OMS	Farm Credit Administration's Office of Management Services
PCIE	President's Council on Integrity and Efficiency
PII	personally identifiable information
POA&M	plan of action and milestones
PPM	Policies and Procedures Manual
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