OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2011 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Management Act

November 15, 2011

E-11-01

Tammy Rapp
Auditor-in-Charge

FARM CREDIT ADMINISTRATION

Memorandum

Office of Inspector General
1501 Farm Credit Drive
McLean, Virginia 22102-5090

FCA
FARM CREDIT ADMINISTRATION

November 15, 2011

The Honorable Leland A. Strom, Chairman and Chief Executive Officer
The Honorable Kenneth A. Spearman, Board Member
The Honorable Jill Long Thompson, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Chairman Strom and Board Members Spearman and Long Thompson:

The Office of the Inspector General completed the 2011 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, and we 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

Carl A. Clinefelter
Inspector General

Office of Inspector General Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Management Act

2011

Report #E-11-01

Farm Credit Administration
Office of Inspector General

November 15, 2011

OIG Evaluation: FISMA 2011

- Introduction and Background
- Objectives, Scope, and Methodology
- Overall Conclusion
- Areas Evaluated by Offices of Inspector General (OIG) During FY 2011
    1. Risk Management
    2. Configuration Management
    3. Incident Response and Reporting
    4. Security Training
    5. Plans of Actions and Milestones (POA&M)
    6. Remote Access Management
    7. Identity and Access Management
    8. Continuous Monitoring Management
    9. Contingency Planning
    10. Contractor Systems
    11. Security Capital Planning
- Appendix A: IG Section Report for Office of Management and Budget (OMB)

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. Title III permanently reauthorized the Government Information Security Reform Act of 2000 and renamed it the Federal Information Security Management Act (FISMA) of 2002. The purpose of FISMA was to strengthen the security of the Federal government's information systems and develop minimum standards for agency systems.
- FISMA requires an agency's Chief Information Officer (CIO) and OIG to conduct annual assessments of the agency's information security program.
- OMB issued Memorandum M-11-33, FY 2011 Reporting Instructions for the FISMA and Agency Privacy Management, on September 14, 2011. This memorandum provides instructions for complying with FISMA's annual reporting requirements and reporting on the agency's privacy management program.
- Results of the CIO and OIG assessments are reported to the OMB thru CyberScope.
- Appendix A contains the IG Section Report as submitted to OMB thru CyberScope.

Objectives, Scope, and Methodology

- The objectives of this evaluation were to perform an independent assessment of the Farm Credit Administration's (FCA or Agency) information security program and assess FCA's compliance with FISMA.
- The scope of this evaluation covered FCA's Agency-owned and contractor operated information systems of record as of September 30, 2011. FCA is a single program Agency with seven mission critical systems and major applications.
- The evaluation covered the eleven areas identified by OMB for OIGs to evaluate.
- 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, IT Security Specialist, Technology Team Leader, Applications Team Leaders, and several IT Specialists;
  - Built on our understanding from past FISMA evaluations;
  - Observed security related activities performed by Agency personnel; and
  - Performed tests for a subset of controls.

Objectives, Scope, and Methodology

- This evaluation represents the status of the information security program as of September 30, 2011, and did not include a test of all information security controls.
- The evaluation was performed at FCA Headquarters in McLean, Virginia, from September 2011 through November 2011.
- Observations and results were shared with key information technology (IT) personnel throughout the evaluation. On November 4, 2011, the CIO and OIG shared and discussed drafts of their respective FISMA section reports.
- An exit conference was conducted with management officials on November 10, 2011.
- This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Overall Conclusion

FCA has an effective information security program that continues to mature and contains the following elements:

- Information security policies and procedures
- Capital planning and investment process that incorporates information security requirements
- Risk based approach to information security
- Systems categorized based on risk
- Security plans that are reviewed and revised regularly
- Risk based security controls implemented
- Security authorization process
- Common security configuration
- Continuous monitoring
- Security awareness and training program
- Continuity of operations plan and tests
- Incident response program
- Oversight of contractor systems

Overall Conclusion

- Engaged CIO, and experienced and well trained IT team
- 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.
- Of the 11 areas OMB required OIGs to evaluate during 2011, FCA has established a program in each of the areas that is consistent with NIST's and OMB's guidelines.
- In FY 2010, there was 1 area that needed improvement and resulted in an agreed-upon action to develop an implementation plan for the United States Government Configuration Baseline (USGCB). FCA made significant progress during FY 2011 to research, test, implement, and document deviations from the USGCB. The CIO plans to be in compliance with the USGCB by June 29, 2012.

Risk Management

FCA established and maintained a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The risk management program includes the following attributes:

- Policy that general support system and major applications will operate with proper accreditation and undergo reauthorization every 3 years or when a major system change occurs
- Addresses risk from organization, mission, business, and information system perspectives
- Information systems categorized based on FIPS 199 and SP 800-60
- Security plans based on risk that identify minimum baseline controls selected, documented, and implemented
- Periodic assessments of controls through a combination of continuous monitoring, self-assessments, independent penetration tests, and security certifications
- Authorizing official considers items identified during the certification process and ensures appropriate action will be taken before signing the "Authorization to Operate"
- Regular communications with senior management

Configuration Management

The Agency established and is maintaining a configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. FCA's security configuration management program includes the following attributes:

- Documented policies and procedures for configuration management
- Standard baseline configuration for workstations and servers
- Regular scanning for compliance and vulnerabilities within the baseline configuration
- Timely remediation of identified vulnerabilities
- Process for timely and secure installation of software patches
- Monitors and analyzes critical security alerts to determine potential impact to FCA systems

As a result of the OIG evaluation during FY 2010, FCA developed an implementation plan to assist in achieving compliance with the USGCB. FCA made significant progress during FY 2011 and has implemented over 70% of USGCB settings on user workstations.

Incident Response and Reporting

The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The incident response and reporting program includes the following attributes:

- Documented policies and procedures, security awareness training and articles, and a 24 hour Helpline for incidents available to employees needing incident assistance.
- Agency staff must report within one hour to the OMS Helpline any IT equipment, personally identifiable information (PII), or sensitive information that is suspected to be missing, lost, or stolen.
- During FY 2011, FCA had the following types of incidents:
  - Malware on laptops
  - Unauthorized computers connected to the network
  - Unauthorized USB devices
  - Phishing email attempts
  - Misplaced or lost HSPD 12 cards, smart phones, USB drives, and laptops (Several lost items were recovered.)
- An analysis was performed for each incident before responding appropriately and timely to minimize further damage.
- A log was maintained of security incidents, and appropriate officials were notified depending on the nature of the incident.

Security Training

The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The security training program includes the following attributes:

- Mandatory annual security awareness training for employees and contractors using small group sessions
    - Revisions to significant security policy
    - Employee and contractor responsibilities
    - Safeguard PII and sensitive information from unauthorized disclosure
    - Modifications to hardware and software require CIO approval
    - Protect laptop and passwords
    - Suspicious email and phishing attempts
    - Prohibited activities
    - Incident reporting
- Security training presentation at new employee orientation
- New employees and contractors required to certify they have read and understood FCA's computer security policies and responsibilities
- Ongoing awareness program that includes e-mails and news alerts with security tips and notices of new threats
- Individual development plan (IDP) process used to identify specialized training for users with significant security responsibilities
- Identification and tracking of employees requiring mandatory and specialized security training

Plans of Actions & Milestones (POA&M)

The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. The POA&M program includes the following attributes:

- Policy for developing plans of action and milestones
- Process for developing plans of corrective action for significant information security weaknesses and tracking their implementation
- Compensating controls currently in place until outstanding items are remediated

Remote Access Management

The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The remote access program includes the following attributes:

- Policies and procedures for authorizing, monitoring, and controlling all methods of remote access
- Virtual private network (VPN) for secure encrypted transmission of data outside of the Agency's network
- Encryption on local hard drives and USB drives to protect sensitive data and PII
- Forced encryption when creating CDs and DVDs
- Security policy and device management for Agency smart phones and authorized personal devices
- Remote contractor access for diagnostic purposes tightly controlled and closely supervised by IT staff

Identity and Access Management

The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. The account and identity management program includes the following attributes:

- Documented policies and procedures for requesting, issuing, and closing information system accounts
- Identifies and authenticates information system users before allowing access
- Detects unauthorized devices and disables connectivity
- Dual-factor authentication
- Information system accounts created, managed, monitored, and disabled by authorized personnel
- Periodic review of information system accounts to ensure access permissions provided to users is current and appropriate
- Controls to prevent, detect, or notify authorized personnel of suspicious account activity or devices

Continuous Monitoring Management

The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The continuous monitoring program includes the following attributes:

- Continuous monitoring strategy reflected in Infrastructure Security Plan and Management Control Plan
- Malicious code protection
- Vulnerability scanning
- Log monitoring
- Notification of unauthorized devices
- Notification of changes or additions to sensitive accounts
- Ongoing monitoring of security alerts and updates from vendors and appropriate action in response
- Commitment to annual independent penetration test

Contingency Planning

The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The contingency planning program includes the following attributes:

- Business continuity plan and disaster recovery plan periodically updated to support the restoration of operations and systems after a disruption or failure
- Alternative processing site and essential systems successfully activated during a government wide test
- Backup strategy includes daily and weekly backups of data and systems
- Three off-site storage facilities for backups
- Disaster recovery kit maintained offsite that contains critical software needed to recreate systems
- Employee notification system used to alert employees of office closing and other events

Contractor Systems

The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. The contractor system oversight program includes the following attributes:

- Written agreements for all contractor systems and interconnections
- Updates inventory of contractor systems and interconnections annually
- Reviews and updates security plans for contractor systems annually
- Performed due diligence reviews and monitored security controls for outsourced systems
- Performed site visits to review security documentation and verify financial and personnel system providers employed adequate security measures to protect information, applications, and services
- Periodically reviewed user accounts and privileges

Security Capital Planning

The Agency has established and maintains a security capital planning and investment program for information security. The program includes the following attributes:

- Policies and procedures that stress importance of information security and protecting sensitive information
- Capital planning and investment process that incorporates information security requirements
- Enterprise architecture that ensures IT investments support core business functions and provides security standards

Inspector General

Section Report

2011

Annual FISMA Report

Farm Credit Administration

Section 1: Risk Management

1a. **The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

1.a(1). **Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.**

Yes

1.a(2). **Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1**

Yes

1.a(3). **Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.**

Yes

1.a(4). **Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.**

Yes

1.a(5). **Categorizes information systems in accordance with government policies.**

Yes

1.a(6). **Selects an appropriately tailored set of baseline security controls.**

Yes

1.a(7). **Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**

Yes

1.a(8). **Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.**

Yes

1.a(9). **Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that**

Section 1: Risk Management

this risk is acceptable.

Yes

1.a(10). Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Yes

1.a(11). Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

Yes

1.a(12). Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

Yes

1.a(13). Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

Yes

1.a(14). Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.

Yes

Section 2: Configuration Management

2.a. The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

2.a(1). Documented policies and procedures for configuration management.

Yes

2.a(2). Standard baseline configurations defined.

Yes

2.a(3). Assessing for compliance with baseline configurations.

Section 2: Configuration Management

Yes

2.a(4). **Process for timely, as specified in Agency policy or standards, remediation of scan result deviations.**

Yes

2.a(5). **For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.**

No

Comments:

Although FDCC/USGCB secure configuration settings are not fully implemented, FCA has made significant progress in the past year.

FCA's current USGCB status:
- implemented over 70% of USGCB settings;
- continues to research and test outstanding settings; and
- documented and approved 17 deviations by the CIO.

2.a(6). **Documented proposed or actual changes to hardware and software configurations.**

Yes

2.a(7). **Process for timely and secure installation of software patches.**

Yes

Section 3: Incident Response and Reporting

3a. **The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

3a(1). **Documented policies and procedures for detecting, responding to and reporting incidents.**

Yes

3a(2). **Comprehensive analysis, validation and documentation of incidents.**

Yes

3a(3). **When applicable, reports to US-CERT within established timeframes.**

Section 3: Incident Response and Reporting

Yes

3a(4). **When applicable, reports to law enforcement within established timeframes.**

Yes

3a(5). **Responds to and resolves incidents in a timely manner, as specified in Agency policy or standards, to minimize further damage.**

Yes

3a(6). **Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.**

Yes

3a(7). **Is capable of correlating incidents.**

Yes

Section 4: Security Training

4.a. **The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

4.a(1). **Documented policies and procedures for security awareness training.**

Yes

4.a(2). **Documented policies and procedures for specialized training for users with significant information security responsibilities.**

Yes

4.a(3). **Security training content based on the organization and roles, as specified in Agency policy or standards.**

Yes

4.a(4). **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Agency users) with access privileges that require security awareness training.**

Yes

4.a(5). **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Agency users) with significant information security responsibilities that require specialized training.**

Yes

Section 4: Security Training

Section 5: POA&M

5.a. The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

5.a(1). Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

Yes

5.a(2). Tracks, prioritizes and remediates weaknesses.

Yes

5.a(3). Ensures remediation plans are effective for correcting weaknesses.

Yes

5.a(4). Establishes and adheres to milestone remediation dates.

Yes

5.a(5). Ensures resources are provided for correcting weaknesses.

Yes

5.a(6). Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

Yes

Section 6: Remote Access Management

6.a. The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

6.a(1). Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.

Yes

6.a(2). Protects against unauthorized connections or subversion of authorized connections.

Section 6: Remote Access Management

Yes

6.a(3). Users are uniquely identified and authenticated for all access.

Yes

6.a(4). If applicable, multi-factor authentication is required for remote access.

Yes

6.a(5). Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

6.a(6). Defines and implements encryption requirements for information transmitted across public networks.

Yes

6.a(7). Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.

Yes

Section 7: Identity and Access Management

7.a. The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

7.a(1). Documented policies and procedures for account and identity management.

Yes

7.a(2). Identifies all users, including federal employees, contractors, and others who access Agency systems.

Yes

7.a(3). Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

7.a(4). If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.

Yes

Section 7: Identity and Access Management

7.a(5). **Ensures that the users are granted access based on needs and separation of duties principles.**

Yes

7.a(6). **Identifies devices that are attached to the network and distinguishes these devices from users.**

Yes

7.a(7). **Ensures that accounts are terminated or deactivated once access is no longer required.**

Yes

7.a(8). **Identifies and controls use of shared accounts.**

Yes

Section 8: Continuous Monitoring Management

8.a. **The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

8.a(1). **Documented policies and procedures for continuous monitoring.**

Yes

8.a(2). **Documented strategy and plans for continuous monitoring.**

Yes

8.a(3). **Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.**

Yes

8.a(4). **Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans.**

Yes

Section 9: Contingency Planning

9.a. **The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with**

Section 9: Contingency Planning

FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

9.a(1). Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

Yes

9.a(2). The Agency has performed an overall Business Impact Analysis (BIA).

Yes

9.a(3). Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

Yes

9.a(4). Testing of system specific contingency plans.

Yes

9.a(5). The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

Yes

9.a(6). Development of test, training, and exercise (TT&E) programs.

Yes

9.a(7). Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

Yes

Section 10: Contractor Systems

10.a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

10.a(1). Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(2). The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and

Section 10: Contractor Systems

comply with federal and Agency guidelines.

Yes

10.a(3). A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(4). The inventory identifies interfaces between these systems and Agency-operated systems.

Yes

10.a(5). The Agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.a(6). The inventory of contractor systems is updated at least annually.

Yes

10.a(7). Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Section 11: Security Capital Planning

11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

11.a(1). Documented policies and procedures to address information security in the capital planning and investment control process.

Yes

11.a(2). Includes information security requirements as part of the capital planning and investment process.

Yes

11.a(3). Establishes a discrete line item for information security in organizational programming and documentation.

Yes

11.a(4). Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.

Yes

Section 11: Security Capital Planning

11.a(5). Ensures that information security resources are available for expenditure as planned.

Yes