OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2012 Evaluation of the
Farm Credit Administration's
Compliance with the
Federal Information Security
Management Act

November 9, 2012

E-12-01

Tammy Rapp
Auditor-in-Charge

FARM CREDIT ADMINISTRATION

Memorandum

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

November 9, 2012

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 2012 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 2012

Report #E-12-01

Farm Credit Administration
Office of Inspector General

November 9, 2012

OIG Evaluation: FISMA 2012 Outline

Introduction and Background
Objectives, Scope, and Methodology
Overall Conclusion
Areas Evaluated by Offices of Inspector General (OIG) During FY 2012

1. Continuous Monitoring Management
2. Configuration Management
3. Identity and Access Management
4. Incident Response and Reporting
5. Risk Management
6. Security Training
7. Plans of Actions and Milestones (POA&M)
8. Remote Access 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-12-20, FY 2012 Reporting Instructions for the FISMA and Agency Privacy Management, on October 2, 2012. 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, 2012. FCA is a single program Agency with nine mission critical systems and major applications.

The evaluation covered the eleven areas identified by the Department of Homeland Security (DHS) for OIGs to evaluate.

Key criteria used to evaluate FCA's information security program and compliance with FISMA included OMB and DHS 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 Leader, Client Services and Communications Team Leader, 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, 2012, and did not include a test of all information security controls.

The evaluation was performed at FCA Headquarters in McLean, Virginia, from September 2012 through November 2012.

Observations and results were shared with key information technology (IT) personnel throughout the evaluation. On November 9, 2012, the CIO and OIG shared and discussed drafts of their respective FISMA section reports.

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
- Risk based approach to information security
- Systems categorized based on risk
- Risk based security controls implemented
- Security authorization process
- Continuous monitoring
- Standard baseline configurations
- Identity and access management program
- Remote access controls
- Security awareness and training program
- Incident response program
- Continuity of operations plan and tests
- Oversight of contractor systems
- Capital planning and investment process that incorporates information security requirements

Overall Conclusion

FCA has an engaged CIO with an experienced and well trained IT team. 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.

Of the 11 areas OMB required OIGs to evaluate during 2012, FCA has established a program in each of the areas that is consistent with NIST's and OMB's guidelines.

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 with appropriate action
- Commitment to annual independent penetration test
- Annual internal controls assessment

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 vulnerabilities and compliance within the baseline configuration
- Controls to prevent unauthorized software
- Controls to prevent unauthorized devices
- Timely remediation of identified vulnerabilities
- Process for timely and secure installation of software patches
- Monitoring and analysis of critical security alerts to determine potential impact to FCA systems
- Implementation of the USGCB with deviations approved by the CIO

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 identity and access 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
- Strengthened controls over use of elevated privileges
- 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, and notify authorized personnel of suspicious account activity or devices

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
- Significant improvement in the timeliness of incident reporting by users during FY 2012
- During FY 2012, FCA had the following types of incidents:
  - Malware on laptops
  - Unauthorized computers detected and removed from the Agency's network
  - Unauthorized scans and attempted unauthorized access blocked from the Agency's network
  - Phishing email attempts
  - Stolen laptop, HSPD 12 card, and smart phone
  - Misplaced or lost HSPD 12 cards and smart phones (Several lost phone were recovered.)
- Analysis was performed for each incident before responding appropriately and timely to minimize further damage
- Log was maintained of security incidents, and appropriate officials were notified depending on the nature of the incident

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

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
  - Importance of HSPD 12 cards
  - Preventing and reacting to a virus
  - Personal use of agency devices
  - Social media
  - Password management
  - Proper care of IT equipment
  - 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 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
- Protection against unauthorized connections
- 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

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
- Off-site storage 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
- Information security resources are available as planned