OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2010 Evaluation of the
Farm Credit Administration's
Compliance with the
Federal Information Security
Management Act

November 15, 2010

E-10-01

Tammy Rapp
Auditor-in-Charge

FARM CREDIT ADMINISTRATION

Memorandum

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

November 15, 2010

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 2010 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 did note one area where improvement can be made, and the Office of Management Services (OMS) agreed to take action on our proposed recommendation. As a result, the recommendation has been changed to an agreed-upon action as follows:

- OMS will develop an action plan to guide the Agency in achieving compliance with the United States Government Configuration Baseline.

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

Respectfully,

Carl A. Clinefelter
Inspector General

Office of Inspector General Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Management Act 2010

Report #E-10-01

Farm Credit Administration
Office of Inspector General

November 15, 2010

OIG Evaluation: FISMA 2010

- Introduction and Background
- Objectives, Scope, and Methodology
- Overall Conclusion
- Areas Evaluated by Offices of Inspector General (OIG) During FY 2010
  1. Certification and Accreditation Program
  2. Security Configuration Management
  3. Incident Response and Reporting Program
  4. Security Training Program
  5. Plans of Actions and Milestones (POA&M) Program
  6. Remote Access Program
  7. Account and Identity Management Program
  8. Continuous Monitoring Program
  9. Contingency Planning Program
  10. Agency Program to Oversee Contractor Systems
- 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-10-15, FY 2010 Reporting Instructions for the FISMA and Agency Privacy Management, on April 21, 2010. This memorandum provides instructions for complying with FISMA's annual reporting requirements and reporting on the agency's privacy management program. OMB made significant changes to this year's reporting metrics for the CIO, Privacy Officer, and OIG.
- 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, 2010. FCA is a single program Agency with seven mission critical systems.
- The evaluation covered the ten 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 and other key personnel;
  - 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, 2010, and did not include a test of all information security controls.
- The evaluation was performed at FCA Headquarters in McLean, Virginia, from September 2010 through November 2010.
- Observations and results were presented to key information technology (IT) personnel throughout the evaluation. On November 9, 2010, 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, 2010.
- This evaluation was performed in accordance with the former President's Council on Integrity and Efficiency's[1] *Quality Standards for Inspections* .

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

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
  - Enterprise architecture that ensures IT investments support core business functions and provides security standards
  - 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 program
  - Continuity of operations plan and tests
  - Incident response program
- 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.

Overall Conclusion

- Of the 10 areas OMB required OIGs to evaluate during 2010, FCA has established a program in 9 of the areas that is generally consistent with NIST's and OMB's requirements.
- Although 1 area needing improvement resulted in an agreed-upon action, FCA has compensating controls in place to minimize the likelihood of an adverse event.

Certification and Accreditation Program

- FCA established and maintained a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. The certification and accreditation program includes the following elements:
  - The Agency's policy states the general support system and major applications will operate with proper accreditation and undergo recertification every 3 years or when a major system change occurs.
  - Accreditation boundaries defined in security plans
  - 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"

Security Configuration Management

- The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make improvements.
- 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
  - Process for timely and secure installation of software patches
  - Monitors and analyzes critical security alerts to determine potential impact to FCA systems
- However, FCA has not implemented the Federal Desktop Core Configuration (FDCC) and not fully documented all deviations. The FDCC provides the baseline security settings that Federal agencies are required to implement and was replaced in May 2010 by the United States Government Configuration Baseline (USGCB).
  - Agreed-upon Action:
    1. FCA should develop an action plan to guide the Agency in achieving compliance with the FDCC/USGCB. The action plan should address the following:
       - Schedule for completion with key milestones
       - Adopt remaining FDCC/USGCB settings and document approved deviations
       - Periodically monitor compliance with the FDCC/USGCB and approved deviations

Incident Response and Reporting Program

- The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. The incident response and reporting program includes the following elements:
  - Documented policies and procedures, security awareness training and articles, wallet cards with help desk contact information, and a 24 hour Helpline for incidents are 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 2010, incidents included instances of malware on laptops, unauthorized USB devices, lost HSPD 12 cards, smart phones, and laptops.
  - 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 Program

- The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. The security training program includes the following elements:
  - Ongoing IT security awareness program
  - Mandatory annual security awareness training for employees and contractors using small group sessions
    - Reminded employees and contractors of their responsibilities
    - E-mail confidentiality footers
    - Encrypted e-mail
    - Web 2.0
    - Peer-to-peer file sharing
    - Phishing
    - Incident reporting
    - Preparing for 2-factor authentication
    - Periodically sent e-mails and news alerts that contain security tips and notices of new threats
    - IT Security Specialist made a presentation at the new employee orientation
  - New employees and contractors required to certify they have read and understood FCA's computer security policies and responsibilities
  - When revised security policies are issued, all users will recertify their understanding of the revised polices
  - Individual development plan (IDP) process used to identify specialized training for users with significant security responsibilities
  - Identification and tracking of employees requiring security training

Plans of Actions & Milestones (POA&M)

- The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. The POA&M program includes the following elements:
  - 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 Program

- The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. The remote access program includes the following elements:
  - Virtual private network (VPN) provides for secure encrypted transmission of data outside of the Agency's network
  - Encryption on local hard drives and USB drives used to protect sensitive data and PII
  - CD/DVD writing is disabled
  - Remote contractor access for diagnostic purposes tightly controlled and closely supervised by IT staff

Account and Identity Management Program

- The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. The account and identity management program includes the following elements:
  - Documented policies and procedures for requesting, issuing, and closing information system accounts
  - Identifies and authenticates information system users and devices before allowing access
  - 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
  - Planning and preparation for dual-factor authentication with the roll-out of new laptops during 2011

Continuous Monitoring Program

- The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. The continuous monitoring program includes the following elements:
  - Infrastructure Security Plan and Management Control Plan reflect continuous monitoring strategy
  - 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 Program

- The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. The contingency planning program includes the following elements:
  - FCA committed resources to ensure the continuity of operations of essential functions in emergency situations
  - Business continuity plan and disaster recovery plan were developed and periodically updated to support the restoration of operations and systems after a disruption or failure
  - Alternative processing site and essential systems successfully activated during a government wide test
  - Backup strategy includes daily and weekly backups of data and systems
  - Two 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
  - Many FCA employees successfully continued to work remotely from their homes when the office was closed during a snow emergency

Agency Program to Oversee Contractor Systems

- The Agency has established and maintains a program to oversee systems operated on its behalf by contractors. The contractor system oversight program includes the following elements:
  - Memorandum of Understanding, Interconnect Service Agreement, Contract, or Agreement 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

Inspector General

Section Report

2010

Annual FISMA Report

Farm Credit Administration

Printed: November 10, 2010, 10:06 am

Section 1: Status of Certification and Accreditation Program

1. Selected response is:

a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.

2. Establishment of accreditation boundaries for agency information systems.

3. Categorizes information systems.

4. Applies applicable minimum baseline security controls.

5. Assesses risks and tailors security control baseline for each system.

6. Assessment of the management, operational, and technical security controls in the information system.

7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.

8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.

Section 2: Status of Security Configuration Management

2. Selected response is:

b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.

2a. Areas for Improvement:

2a(1). Configuration management policy is not fully developed.

No

2a(2). Configuration management procedures are not fully developed or consistently implemented.

No

2a(3). Software inventory is not complete (NIST 800-53: CM-8).

No

Section 2: Status of Security Configuration Management

2a(4). Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).

No

2a(5). Hardware inventory is not complete (NIST 800-53: CM-8).

No

2a(6). Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).

No

2a(7). Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).

No

2a(8). FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.

Yes

Comments: FCA is in the process of consolidating FDCC and existing group policies to eliminate any redundancy in the group policies. FCA has agreed to develop an action plan to guide the Agency in achieving compliance with the FDCC/USGCB.

2a(9). Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).

No

2a(10). Configuration-related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).

No

2a(11). Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).

No

2a(12). Other

No

3. Identify baselines reviewed:

Operating System
Microsoft Windows Vista Enterprise Edition

Section 3: Status of Incident Response & Reporting Program

4. Selected response is:

Section 3: Status of Incident Response & Reporting Program

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

1. Documented policies and procedures for responding and reporting to incidents.
2. Comprehensive analysis, validation and documentation of incidents.
3. When applicable, reports to US-CERT within established timeframes.
4. When applicable, reports to law enforcement within established timeframes.
5. Responds to and resolves incidents in a timely manner to minimize further damage.

Section 4: Status of Security Training Program

5. Selected response is:

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

1. Documented policies and procedures for security awareness training.
2. Documented policies and procedures for specialized training for users with significant information security responsibilities.
3. Appropriate training content based on the organization and roles.
4. Identification and tracking of all employees with login privileges that need security awareness training.
5. Identification and tracking of employees without login privileges that require security awareness training.
6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

6. Selected response is:

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

1. Documented policies and procedures for managing all known IT security weaknesses.
2. Tracks, prioritizes and remediates weaknesses.
3. Ensures remediation plans are effective for correcting weaknesses.
4. Establishes and adheres to reasonable remediation dates.
5. Ensures adequate resources are provided for correcting weaknesses.
6. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

CIO centrally tracks, maintains, and independently reviews/validates the POAM activities at least quarterly.

Section 6: Status of Remote Access Program

7. Selected response is:

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

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

2. Protects against unauthorized connections or subversion of authorized connections.

3. Users are uniquely identified and authenticated for all access.

4. If applicable, multi-factor authentication is required for remote access.

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

6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.

7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.

Section 7: Status of Account and Identity Management Program

8. Selected response is:

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

1. Documented policies and procedures for account and identity management.

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

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

4. If multi-factor authentication is in use, it is linked to the Agency's PIV program.

5. Ensures that the users are granted access based on needs and separation of duties principles.

6. Identifies devices that are attached to the network and distinguishes these devices from users.

7. Ensures that accounts are terminated or deactivated once access is no longer required.

Section 8: Status of Continuous Monitoring Program

Section 8: Status of Continuous Monitoring Program

9. Selected response is:

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

1. Documented policies and procedures for continuous monitoring.

2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.

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

4. Provides system 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.

Section 9: Status of Contingency Planning Program

10. Selected response is:

a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

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

2. The agency has performed an overall Business Impact Assessment.

3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

4. Testing of system specific contingency plans.

5. The documented business continuity and disaster recovery plans are ready for implementation.

6. Development of training, testing, and exercises (TT&E) approaches.

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

Section 10: Status of Agency Program to Oversee Contractor Systems

11. Selected response is:

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

1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors

Section 10: Status of Agency Program to Oversee Contractor Systems

or other entities the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.

2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.

3. The inventory identifies interfaces between these systems and Agency-operated systems.

4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that is owns and operates.

5. The inventory, including interfaces, is updated at least annually.

6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.