OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2015 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

E-15-01

Auditor-in-Charge
Tammy Rapp

Issued November 13, 2015

FARM CREDIT ADMINISTRATION

Memorandum

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

November 13, 2015

The Honorable Kenneth A. Spearman, Board Chairman
The Honorable Dallas P. Tonsager, Board Member
The Honorable Jeffery S. Hall, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Board Chairman Spearman and FCA Board Members Tonsager and Hall:

The Office of the Inspector General (OIG) completed the 2015 independent evaluation of the Farm Credit Administration's (FCA) compliance with the Federal Information Security Modernization 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 information security program that continues to mature. Of the ten areas the Office of Management and Budget required OIGs to evaluate during 2015, FCA established a program in all areas. This report contains no recommendations.

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,

Elizabeth M. Dean
Inspector General

Office of Inspector General (OIG) Evaluation: FISMA 2015

Table of Contents

Executive Summary

The Farm Credit Administration (FCA or Agency) has an information security program that continues to mature and contains the following elements:

- Capital planning and investment process that incorporates information security requirements
- Information security policies and procedures
- Risk based approach to information security
- Continuous monitoring
- Standard baseline configurations
- Patch management process
- Vulnerability assessments
- Identity and access management program
- Incident response program
- Implementation of risk based security controls
- Security authorization process
- Security awareness and training program
- Corrective action for significant information security weaknesses
- Remote access controls
- Continuity of operations plan and tests
- Oversight of contractor systems

Executive Summary

- FCA has an experienced information technology (IT) team that is proactive in their approach to information security.
- The IT team and system sponsors were responsive to suggestions made for improvement during the Federal Information Security Modernization Act (FISMA) evaluation and, in many cases, the IT staff made immediate changes to strengthen the information security program.
- Of the ten areas the Office of Management and Budget (OMB) required OIGs to evaluate during 2015, FCA established a program in all of the areas that is consistent with National Institute of Standards and Technology's (NIST), Department of Homeland Security's (DHS), and OMB's guidelines.

Introduction and Background

The President signed into law the FISMA of 2014 on December 18, 2014.

- Amended the Federal Information Security Management Act of 2002.
- The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls, minimum controls for agency systems, and improved oversight of agency information security programs.
- FISMA requires OIGs to perform an annual independent evaluation that includes:
  - testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems, and
  - an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

OMB issued Memorandum M-16-03 on October 30, 2015, with reporting instructions for complying with FISMA's annual reporting requirements and reporting on the agency's privacy management program. Results of the Chief Information Officer (CIO) and OIG assessments are reported to the OMB through CyberScope.

Appendix A of this report contains the IG Section Report as submitted to OMB through CyberScope.

Appendix B of this report describes the objectives, scope, and methodology used for this evaluation.

Continuous Monitoring Management

The Agency's information security continuous monitoring (ISCM) program continues to evolve as new security requirements are developed and resources are available. The Agency is working with DHS to identify and obtain additional ISCM technologies that complement FCA's environment. In the past year, FCA summarized their ISCM strategy and implemented new ISCM tools provided by DHS.

Utilizing the ISCM maturity model definitions, we assessed the maturity of FCA's ISCM program along the domains of people, processes, and technology. We determined FCA's ISCM program is currently a Level 1 in all domains. FCA is working on further defining and implementing its ISCM program, which will increase its maturity level in the future.

FCA's continuous monitoring program currently includes the following attributes:

- ISCM strategy based on risk
- Use of off-the-shelf, custom, and manual monitoring tools supplemented by DHS scanning
- Notification of unauthorized devices and changes or additions to sensitive accounts
- Vulnerability scanning
- Ongoing monitoring of security alerts and updates from vendors and appropriate action
- Commitment to annual independent penetration test and periodic security tests and evaluations of major systems
- Resolving identified weaknesses as quickly as possible

Configuration Management

The Agency established and maintains a configuration management program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

The security configuration management program includes the following attributes:

- Documented policies and procedures for configuration management
- Standard baseline configuration for workstations and servers
- Implementation of the United States Government Configuration Baseline (USGCB)
- Regular scanning of servers 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

Identity and Access Management

The Agency established and maintains an identity and access management program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

The identity and access management program identifies users and network devices and includes the following attributes:

- Documented policies and procedures for requesting, issuing, changing, 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 are current and appropriate
- Controls to prevent, detect, or notify authorized personnel of suspicious account activity or devices

Incident Response and Reporting

The Agency established and maintains an incident response and reporting program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

The incident response and reporting program includes the following attributes:

- Documented policies and procedures
- Security awareness training and articles
- A 24 hour Helpline available to employees needing incident assistance
- A requirement that agency staff report within one hour to the Helpline any IT equipment, personally identifiable information (PII), or sensitive information that is suspected to be missing, lost, or stolen
- During FY 2015, FCA had the following types of incidents:
  - Misplaced or lost HSPD12 cards, smartphones, and tablets
  - Malware on laptops
  - Inadvertent exposure of PII
  - Phishing email attempts
- 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

Risk Management

The Agency established and maintains a risk management program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

The risk management program includes the following attributes:

- Addressed risk from organization, mission, business, and information system perspectives
- Information systems categorized based on Federal Information Processing Standards (FIPS) Publication 199 and Special Publication (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 independent security tests and evaluations
- Authorizing official considered risk of items identified during the certification process before signing the “Authorization to Operate”
- Regular communications with senior management

Security Training

The Agency established and maintains a security training program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

The security training program includes the following attributes:

- Documented policies and procedures for:
  - security awareness that are accessible to employees
  - training for users with significant IT responsibilities
- Mandatory annual security awareness training for all employees and contractors that included:
  - examples of information security threats and incidents that can compromise information security
  - responsibilities federal employees have with regard to maintaining information security
  - security measures and best practices federal employees should use in their everyday work
  - security concerns posed by mobile and remote employees
- Presentation for all new employees when they come on board and at new employee orientation
- Certification by new employees and contractors they have read and understood FCA's computer security policies and responsibilities after meeting with IT Security Specialist
- Ongoing awareness program that includes e-mails and alerts with security tips of new threats
- Ongoing efforts to inform employees of the Office of Personnel Management data breach that affected employees
- Security guidance located on Agency's intranet site that is accessible by all employees
- Specialized training for staff with significant security responsibilities
- Identifying and tracking employees requiring mandatory security training and specialized training

Plans of Action & Milestones (POA&M)

The Agency established and maintains a POA&M program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

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

Remote Access Management

The Agency established and maintains a remote access program that is consistent with FISMA requirements, OMB and DHS 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 to protect sensitive data and personally identifiable information (PII)
- Forced encryption when creating CDs and DVDs
- Security policy and device management for Agency smart phones, tablets, and authorized personal devices
- Remote contractor access for diagnostic purposes tightly controlled and closely supervised by IT staff

Contingency Planning

The Agency established and maintains an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB and DHS policy, and applicable NIST guidelines.

The contingency planning program includes the following attributes:

- Policy and procedures for business continuity and disaster recovery
- Business continuity plan and disaster recovery plan periodically updated to support the restoration of essential operations and systems after a disruption or failure
- Backup strategy includes daily and weekly backups of data and systems
- Off-site storage and encryption for backups
- Alternative processing site with essential systems successfully activated during a government wide test
- Disaster recovery documentation maintained offsite that contains critical software and procedures needed to recreate systems
- A multi-layered communication strategy in place that was tested throughout the year

Contractor Systems

The Agency 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:

- Documented policies and procedures
- Written agreements for contractor systems and interconnections
- Security plans for contractor systems reviewed and updated annually
- Updated inventory of contractor systems and interconnections
- Due diligence reviews performed, and security controls monitored, for the outsourced financial, payroll, and personnel systems
- User accounts and privileges periodically reviewed for outsourced financial, payroll, and personnel systems

Inspector General

Section Report

2015

Annual FISMA Report

Farm Credit Administration

Section 1: Continuous Monitoring Management

1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.

1.1.1 Please provide the D/A ISCM maturity level for the People domain.

Ad Hoc (Level 1)

1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.

Ad Hoc (Level 1)

1.1.3 Please provide the D/A ISCM maturity level for the Technology domain

Ad Hoc (Level 1)

1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.

Ad Hoc (Level 1)

1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.

n/a

Section 2: Configuration Management

2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

2.1.1 Documented policies and procedures for configuration management.

Yes

2.1.2 Defined standard baseline configurations.

Yes

2.1.3 Assessments of compliance with baseline configurations.

Yes

Section 2: Configuration Management

2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings.

Yes

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.

Yes

2.1.6 Documented proposed or actual changes to hardware and software baseline configurations.

Yes

2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).

No

Comments: Servers and network devices are periodically scanned for compliance with the baseline configuration. However, a risk based decision was made to not implement routine scanning of workstations and printers for compliance with FCA's baseline configuration. A cost benefit analysis with consideration of compensating controls was an integral part of the decision.

2.1.8 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).

Yes

2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).

Yes

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

n/a

2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?

No

Comments: Servers and network devices are periodically scanned for compliance with the baseline configuration. However, a risk based decision was made to not implement routine scanning of workstations and printers for compliance with FCA's baseline configuration. A cost benefit analysis with consideration of compensating controls was an integral part of the decision.

Section 2: Configuration Management

2.3.1 **Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.**

Yes

Section 3: Identity and Access Management

3.1 **Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?**

Yes

3.1.1 **Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).**

Yes

3.1.2 **Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2).**

Yes

3.1.3 **Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).**

Yes

3.1.4 **Organization has planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).**

Yes

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

Yes

3.1.6 **Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).**

Yes

3.1.7 **Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.**

Yes

Section 3: Identity and Access Management

3.1.8 Identifies and controls use of shared accounts.

Yes

3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.

n/a

Section 4: Incident Response and Reporting

4.1 Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).

Yes

4.1.2 Comprehensive analysis, validation, and documentation of incidents.

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.1.4 When applicable, reports to law enforcement and the agency Inspector General within established timeframes.

Yes

4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.1.6 Is capable of correlating incidents.

Yes

Section 4: Incident Response and Reporting

4.1.7 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

n/a

Section 5: Risk Management

5.1 Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

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

Yes

5.1.2 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800- 37, Rev. 1.

Yes

5.1.3 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev.1.

Yes

5.1.4 Has an up-to-date system inventory.

Yes

5.1.5 Categorizes information systems in accordance with government policies.

Yes

Section 5: Risk Management

5.1.6 **Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**

Yes

5.1.7 **Implements the approved set of tailored baseline security controls specified in metric 5.1.6.**

Yes

5.1.8 **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

5.1.9 **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 this risk is acceptable.**

Yes

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

Yes

5.1.11 **Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).**

Yes

5.1.12 **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

5.1.13 **Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).**

Yes

5.1.14 **The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.**

Yes

Section 5: Risk Management

5.1.15 For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.

Yes

5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

n/a

Section 6: Security Training

6.1 Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards.

Yes

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

Yes

6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

Yes

6.1.6 Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).

Yes

Section 6: Security Training

6.2 **Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.**

n/a

Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.**

Yes

7.1.2 **Tracks, prioritizes, and remediates weaknesses.**

Yes

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

Yes

7.1.4 **Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.**

Yes

7.1.5 **Ensures resources and ownership are provided for correcting weaknesses.**

Yes

7.1.6 **POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk- based decision to not implement a security control) (OMB M-04-25).**

Yes

7.1.7 **Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).**

Yes

Section 7: Plan Of Action & Milestones (POA&M)

7.1.8 **Program officials 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 (NIST SP 800-53:CA-5; OMB M-04-25).**

Yes

7.2 **Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.**

n/a

Section 8: Remote Access Management

8.1 **Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

8.1.1 **Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).**

Yes

8.1.2 **Protects against unauthorized connections or subversion of authorized connections.**

Yes

8.1.3 **Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).**

Yes

8.1.4 **Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).**

Yes

8.1.5 **Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.**

Yes

8.1.6 **Defines and implements encryption requirements for information transmitted across public networks.**

Yes

Section 8: Remote Access Management

8.1.7 **Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.**

Yes

8.1.8 **Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).**

Yes

8.1.9 **Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).**

Yes

8.1.10 **Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).**

Yes

8.2 **Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.**

n/a

8.3 **Does the organization have a policy to detect and remove unauthorized (rogue) connections?**

Yes

Section 9: Contingency Planning

9.1 **Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

9.1.1 **Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).**

Yes

Section 9: Contingency Planning

9.1.2 **The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).**

Yes

9.1.3 **Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).**

Yes

9.1.4 **Testing of system-specific contingency plans.**

Yes

9.1.5 **The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).**

Yes

9.1.6 **Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.7 **Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.**

Yes

9.1.8 **After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).**

Yes

9.1.9 **Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.10 **Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.11 **Contingency planning that considers supply chain threats.**

Yes

Section 9: Contingency Planning

9.2 **Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.**

n/a

Section 10: Contractor Systems

10.1 **Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

10.1.1 **Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.**

Yes

10.1.2 **The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).**

Yes

10.1.3 **A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.**

Yes

10.1.4 **The inventory identifies interfaces between these systems and organization- operated systems (NIST SP 800-53: PM-5).**

Yes

10.1.5 **The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.**

Yes

10.1.6 **The inventory of contractor systems is updated at least annually.**

Yes

Section 10: Contractor Systems

10.2 **Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.**

n/a

Appendix B: Objectives, Scope, and Methodology

- The objective of this evaluation was to perform an independent assessment of FCA's information security program by assessing the agency's performance of ten areas identified by DHS.
- The scope of this evaluation covered FCA's Agency-owned and contractor operated information systems of record as of September 30, 2015. FCA is a single program Agency with eight mission critical systems and major applications.
- Key criteria used to evaluate FCA's information security program and compliance with FISMA included OMB and DHS guidance, NIST SPs, and 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, Information Technology Security Specialist, Associate Director Technology Team, Associate Director Applications Team, 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.
- This evaluation represents the status of the information security program as of September 30, 2015, and did not include a test of all information security controls.
- The evaluation was performed at FCA Headquarters in McLean, Virginia, from September 2015 through November 2015.

Appendix B: Objectives, Scope, and Methodology

- Observations and results were shared with key IT personnel throughout the evaluation.
- On November 10, 2015, the CIO, Information Technology Security Specialist, 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*.

REPORT

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