OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2016 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

E-16-01

Evaluator-in-Charge
Tammy Rapp

Evaluator
Sonya Cerne

Issued November 10, 2016

FARM CREDIT ADMINISTRATION

Memorandum

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

November 10, 2016

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 2016 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 FCA has an information security program that continues to mature. FCA's overall information security program scored 70 points out of 100 possible points. Although FCA's information security program was not ranked "Effective" based on the Department of Homeland Security's scoring methodology, we did not make any recommendations because FCA continues to identify areas to strengthen and improve information security.

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:

Federal Information Security Modernization Act (FISMA) - 2016

Table of Contents

Executive Summary

The Farm Credit Administration (FCA or Agency) has an information security program that continues to mature. FCA's overall information security program scored 70 points out of 100 possible points. Although FCA's information security program was not ranked "Effective"[1] based on the Department of Homeland Security's (DHS) scoring methodology, we did not make any recommendations because FCA continues to identify areas to strengthen and improve information security.

The table below summarizes the results from CyberScope's scoring. Each information security function area is discussed in more detail in the body of this report.

Information Security Function Area	**Ranking assigned by CyberScope**
Identify	Level 4: Managed and Measurable
Protect	Level 4: Managed and Measurable
Detect	Level 2: Defined
Respond	Level 2: Defined
Recover	Level 5: Optimized

[1] See Introduction and Background for information regarding DHS' scoring methodology.

Executive Summary

FCA's information security program contains the following elements:

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

FCA has an experienced information technology (IT) team who are proactive in their approach to information security. FCA was responsive to suggestions made for improvement during the Federal Information Security Modernization Act of 2014 (FISMA) evaluation, and IT staff agreed to make changes to strengthen the information security program.

Introduction and Background

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

- 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. This includes:
  - testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems, and
  - assessing the effectiveness of the information security policies, procedures, and practices of the agency.

Office of Management & Budget (OMB) issued Memorandum M-17-05 on November 4, 2016, with guidance 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.

As with the FY 2016 CIO FISMA Reporting Metrics, the IG metrics are organized around the five information security functions outlined in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of

Introduction and Background

controls to address those risks. There are eight domains represented within the five information security functions outlined in the Cybersecurity Framework.

1. Risk Management (Identify)
2. Contractor Systems (Identify)
3. Configuration Management (Protect)
4. Identity and Access Management (Protect)
5. Security and Privacy Training (Protect)
6. Information Security Continuous Monitoring (Detect)
7. Incident Response (Respond)
8. Contingency Planning (Recover)

Starting this year, DHS defined and developed a methodology for determining an "Effective" information security program and "Effective" information security functions.

DHS defined an "Effective" information security program as Level 4, *Managed and Measurable*. CyberScope assigns points and calculates the scores for the five information security functions and the overall information security program. Out of a possible 100 points for the overall information security program, an agency must have 80 points or higher to be considered "Effective."

Introduction and Background

An information security function is defined as "Effective" if it has a level of maturity at or above Level 4, *Managed and Measurable*. To be an "Effective" function, all metrics in Levels 1 through 3 and half or greater of the metrics designated Level 4: Managed and Measurable must be met. All of the metrics in previous levels must be met to move to the next level.

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

Identify

The information security function area for Identify includes the following domains:

- Risk Management
- Contractor Systems

We evaluated the domains in Identify using the guidance provided by DHS. Based on DHS's scoring methodology, FCA has met the criteria for Level 4: Managed and Measurable, which is defined as "Effective." The next two pages provide a summary of the attributes in these respective domains.

Identify: Risk Management

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

The Risk Management program includes the following attributes:

- Comprehensive Agency policies and procedures
- Current system inventory of all major systems including systems residing in the cloud
- Risk addressed from organization, mission, business, and information system perspectives
- Regular and timely communications related to information system security risks with senior management and information system owners
- 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
- Written agreements for contractor systems and direct interfaces
- Periodic assessments of controls through a combination of continuous monitoring, self-assessments, independent penetration tests, and independent security tests and evaluations
- A formal process for authorizing information systems based on acceptable risks
- Policy and procedures for developing plans of action and milestones and tracking their implementation

Identify: 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
- Established and implemented a process to ensure that agreements for systems and services include appropriate information security and privacy requirements
- Specified information security requirements within appropriate agreements for contractors and systems
- Obtained sufficient assurance that the security controls of contractor systems meet FISMA requirements, OMB policy, and applicable NIST guidelines

Protect

The information security function area for Protect includes the following domains:

- Configuration Management
- Identity and Access Management
- Security and Privacy Training

We evaluated the domains in Protect using the guidance provided by DHS. Based on DHS's scoring methodology, FCA has met the criteria for Level 4: Managed and Measurable which is defined as "Effective." The next three pages provide a summary of the attributes in these respective domains.

Protect: Configuration Management

The Agency established and maintains a configuration management program 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
- Procedures for tracking and reporting inventory of Agency's hardware and software
- Standard baseline configuration for workstations and servers
- Controls to prevent unauthorized devices and software
- Identifies, documents, justifies, and approves deviations from standard configuration
- Routine scanning of systems for vulnerabilities and compliance within the baseline configuration
- Timely remediation of identified vulnerabilities
- Process for identification and installation of software patches

Protect: Identity and Access Management

The Agency established and maintains an identity and access management program 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 identity and access management
- Employee certification they have read the Agency's policy on information security
- System access based on least privilege
- Periodic review of information system accounts to ensure access permissions provided to users are current and appropriate
- Personal Identity Verification (PIV) cards for physical access and dual-factor authentication for logical access
- Strengthened controls over use of elevated privileges
- Information system accounts created, managed, monitored, and disabled by authorized personnel
- Alerted of unauthorized devices connected to network
- Detection of unauthorized remote access by utilizing various controls
- Re-authentication and lockout to network after a predefined period
- Controls to prevent, detect, or notify authorized personnel of suspicious account activity or devices

Protect: Security and Privacy Training

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

The security training program includes the following attributes:

- Comprehensive policies and procedures for security awareness and privacy training
- Developed training material for security and privacy awareness training that contained content relative to the Agency
- Evaluated the skills of individuals with significant security and privacy responsibilities and provided additional security and privacy training content and implemented strategies to close identified gaps
- Identified and tracked status of security and privacy awareness training for all information system users requiring security awareness training with appropriate internal processes to detect and correct deficiencies
- Measured the effectiveness of its security and privacy awareness and training program through social engineering exercises

Detect: Continuous Monitoring Management

The information security function area for Detect includes Continuous Monitoring Management. We evaluated this area using the guidance provided by DHS. Based on DHS's scoring methodology, FCA has met the criteria for Level 2: Defined, which is not considered "Effective." Although this area is not considered effective, we did not make any recommendations because FCA progressed from Level 1 last year to Level 2 this year and continues to develop this area.

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. OIT also supplemented its staff with an information security contractor to assist with further development of its ISCM program.

Utilizing DHS's ISCM maturity model definitions and scoring methodology, 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 at Level 2, *Defined*. FCA is working on further defining and developing its ISCM program. This may increase its maturity level in the future.

FCA's ISCM program currently includes the following attributes:

- Assessed skills, knowledge, and resources needed to implement its ISCM program and a plan to close identified gaps
- Defined how ISCM information is shared with individuals with significant security responsibilities

Detect: Continuous Monitoring Management

- Defined a process and consistently captures lessons learned on the effectiveness of its ISCM program and making necessary improvements
- Identified and defined various technologies it plans to utilize for its ISCM program
- Defined how it will use automation to produce an inventory of authorized and unauthorized devices and software on its network and their security configuration

FCA needs to make progress in the following areas in Level 2:

- Document and communicate to ISCM stakeholders their responsibilities related to the ISCM program
- Define how FCA will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements
- Continue to define processes for ISCM areas that will be utilized
- Identify and define performance measures that will be used to assess the effectiveness of the ISCM program

Respond: Incident Response

The information security function area for Respond includes Incident Response. We evaluated this area using the guidance provided by DHS. Based on DHS's scoring methodology, FCA has met the criteria for Level 2: Defined, which is not considered "Effective." Although this area is not considered effective, we did not make any recommendations because FCA continues to develop this area.

The Agency's Incident Response program continues to evolve as new security requirements are developed and resources are available. Utilizing DHS's Incident Response maturity model definitions and scoring methodology, we assessed the maturity of FCA's Incident Response program along the domains of people, processes, and technology. We determined FCA's Incident Response Program is currently at Level 2, *Defined*. FCA is further defining and developing its Incident Response program, which may increase its maturity level in the future.

FCA's Incident Response program currently includes the following attributes:

- Documented policies and procedures
- A 24-hour Help Line available to employees needing incident assistance
- Requirement that Agency staff immediately report to the Help Line any IT equipment, HSPD-12 ID card, physical access card, personally identifiable information (PII), or sensitive information that is suspected to be missing, lost, or stolen
- Collaboration and reporting of security incidents to DHS
- Applied lessons learned to improve security controls and the Incident Response program
- Used a variety of tools to monitor Agency systems

Respond: Incident Response

FCA needs to make progress in the following areas in Level 2:

- Identify and define the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program
- Define plans to develop and maintain a baseline of network operations and expected data flows for users and systems

Recover: Contingency Planning

The information security function area for Recover includes Contingency Planning. We evaluated this area using the guidance provided by DHS. Based on DHS's scoring methodology, FCA has met the criteria for Level 5: Optimized, which is considered "Effective."

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

The contingency planning program includes the following attributes:

- Established policies and procedures for business continuity and disaster recovery
- Developed and facilitated recovery testing, training, and exercise program
- Incorporated the system's business impact analysis in the development of the continuity program
- Business continuity operations and disaster recovery plans are in place, ready to be executed upon if necessary, tested for effectiveness, and updated as needed
- Identified issues needing improvement as a result of business continuity/disaster recovery exercises
- Tested alternative processing and storage sites that are not subject to the same physical risks as the primary site to ensure essential systems were successfully activated
- Conducted backups of information and protected the confidentiality, integrity, and availability of backup information
- Considered supply chain threats in contingency planning

Appendix A: 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 in eight 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, 2016. 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, CISO, Information Technology Security Specialist, Associate Director, Technology Division, Associate Director, Applications Division, 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, 2016, and did not include a test of all information security controls.
- The evaluation was performed at FCA Headquarters in McLean, Virginia, from July 2016 through November 2016.

Appendix A: Objectives, Scope, and Methodology

- Observations and results were shared with key IT personnel throughout the evaluation.
- On November 8, 2016, the CIO, CISO, 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