OFFICE OF INSPECTOR GENERAL

Evaluation Report

OIG 2018 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act
E-18-03

Evaluator-in-Charge
Tammy Rapp

Issued October 31, 2018

Memorandum

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

October 31, 2018

The Honorable Dallas P. Tonsager, Board Chairman
The Honorable Jeffery S. Hall, Board Member
The Honorable Glen R. Smith, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Board Chairman Tonsager and Board Members Hall and Smith:

The Office of Inspector General (OIG) completed the fiscal year 2018 evaluation of the Farm Credit Administration's (FCA or Agency) compliance with the Federal Information Security Modernization Act (FISMA). FISMA requires Inspectors General or an independent external auditor, as determined by the Inspector General of the agency, to perform an annual evaluation of their agency's security program and practices.

The objective of this evaluation is to conduct an independent evaluation of FCA's information security program using the metrics identified by Department of Homeland Security to determine the effectiveness of the information security program and practices.

The OIG found that FCA's information security program is effective and provides reasonable assurance of adequate security. FCA continues to make positive strides in addressing information security weaknesses. However, we identified five actions that the Office of Information Technology agreed to, which will strengthen and improve the Agency's information security and privacy program in the domains of Identity and Access Management and Data Protection and Privacy.

We appreciate the courtesies and professionalism extended by FCA to our senior auditor, Tammy Rapp, during the evaluation. If you have any questions about this evaluation, Tammy and I would be pleased to meet with you at your convenience.

Respectfully,

Wendy R. Laguarda
Inspector General

Office of Inspector General Evaluation:

Federal Information Security Modernization Act - 2018

Table of Contents

Executive Summary

The Farm Credit Administration (FCA or Agency) has an information security program that continues to mature. FCA's information security program is ranked "Effective" based on our analysis of 67 metrics under the Department of Homeland Security's (DHS) scoring methodology.

Results of Office of Inspector General (OIG) assessments are reported in DHS's CyberScope application. The table below summarizes the results from CyberScope's scoring. Each information security function area and domain are discussed in more detail in the body of this report.

Function	Domain	Ranking assigned by CyberScope
Identify	Risk Management	Level 4: Managed and Measurable
Protect		Level 4: Managed and Measurable
Protect	Configuration Management	Level 4: Managed and Measurable
Protect	Identity and Access Management	Level 3: Consistently Implemented
Protect	Data Protection and Privacy	Level 1: Ad Hoc
Protect	Security Training	Level 4: Managed and Measurable
Detect	Information Security Continuous Monitoring (ISCM)	Level 3: Consistently Implemented
Respond	Incident Response	Level 3: Consistently Implemented
Recover	Contingency Planning	Level 4: Managed and Measurable

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
- Change Control Board
- Standard baseline configurations
- Patch management process
- Vulnerability and security control assessments
- Identity and access management program
- Alerts for suspicious activity and devices
- Security and privacy training program
- Prohibition from accessing personal email on agency laptops
- Continuous monitoring
- Weekly security meetings
- Incident response program
- Continuity of operations plan and tests

However, we identified five actions that the Office of Information Technology (OIT) agreed to, which will strengthen and improve the Agency's information security and privacy program in the domains of Identity and Access Management and Data Protection and Privacy.

Acronyms

Agency	Farm Credit Administration
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information System Security Professional
DHS	Department of Homeland Security
FCA	Farm Credit Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
SP	Special Publication
USB	Universal Serial Bus

Introduction and Background

The President signed into law the Federal Information Security Modernization Act (FISMA) of 2014 on December 18, 2014.[1] 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 a representative subset of the agency's information systems and assessing the effectiveness of information security policies, procedures, and practices of the agency.

The Office of Management and Budget (OMB) issued Memorandum M-18-02 on October 16, 2017, with guidance for complying with FISMA's annual reporting requirements. Results of the Chief Information Officer (CIO) and OIG assessments are reported to DHS through CyberScope.

DHS issued the Inspector General FISMA Reporting Metrics on May 24, 2018. The Inspector General Reporting metrics were developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal CIO Council. The fiscal year (FY) 2018 OIG FISMA metrics leverage the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as a standard for managing and reducing cybersecurity risks and are organized around the framework's five functions: Identify, Protect, Detect, Respond, and Recover. Each of the Cybersecurity Framework Security Functions are supported by eight domains. The eight domains contain 67 individual metrics. OIGs evaluate agency progress for each metric. OMB, DHS, and CIGIE worked together over the past few years to transition the metrics into maturity models. During FY 2018, the most significant change to the metrics was the addition of the Data Protection and Privacy domain.

[1] The Government Information Security Reform Act of 2000, which required the first IG evaluations of information security programs, expired in November 2002 and was permanently reauthorized by the Federal Information Security Management Act of 2002. FISMA of 2014 amended the Federal Information Security Management Act of 2002.

Introduction and Background

In FY 2018, DHS's reporting instructions require OIGs to assess agency performance in the following eight domains:

1. Risk Management (Identify)
2. Configuration Management (Protect)
3. Identity and Access Management (Protect)
4. Data Protection and Privacy (Protect)-new domain in FY 2018
5. Security Training (Protect)
6. ISCM (Detect)
7. Incident Response (Respond)
8. Contingency Planning (Recover)

DHS requires OIGs to assess the effectiveness of information security programs and metrics based on a maturity model. Managed and Measurable is considered an effective level of security. The following table describes each maturity level:

Maturity Level	**Maturity Level Description**
Ad-hoc Level 1	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Defined Level 2	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Consistently Implemented Level 3	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable Level 4	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Optimized Level 5	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Introduction and Background

Information Technology (IT) recognized as a Top Management Challenge

IT Security and Management was one of the most frequently reported challenges identified by CIGIE in its report, *Top Management and Performance Challenges Facing Multiple Federal Agencies.* The FCA OIG also identified IT as one of four top management challenges in FCA's FY 2017 Performance and Accountability Report. This challenge is the ability to leverage investments in IT while maintaining a secure environment.

FCA must protect its IT systems and data from the risks of unauthorized access, use, disclosure, disruption, modification, or destruction. While cybersecurity threats are increasing, FCA is increasingly reliant on IT software to identify and analyze potential risks from the sensitive financial data the Agency receives from the Farm Credit System. Hence, it is imperative that FCA has the necessary IT tools and staff to protect its systems and data from cybersecurity threats and to operate more efficiently and effectively. At the same time, the Agency must be prudent and responsible with its spending.

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 domain:

- Risk Management

We evaluated the domain, Identify, using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for **Level 4, Managed and Measurable,** which is defined as effective. The following page provides a summary of the attributes in the Risk Management domain.

Identify: Risk Management

FISMA requires Federal agencies to provide information security protections to agency information and information systems based on a risk-based approach. Specifically, FISMA states that the head of each agency shall provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated on behalf of an agency.

We determined FCA's risk management program is effective based on the risk management metrics developed by DHS and related testing performed during this evaluation. The overall maturity level for FCA's risk management program is **Level 4, Managed and Measurable**.

FCA's risk management strategy focuses on operational risks that may inhibit the ability of its IT assets to support FCA mission-essential functions. FCA's strategy is to use a continuous process of identifying, analyzing, and communicating risks to stakeholders. Risks are identified through various sources such as: continuous monitoring, incident reports, vulnerability scans, assessments, audits, and internal risk assessments.

The Risk Management program includes the following attributes:

- Current system inventory and categorization of all major systems, including systems residing in the cloud
- Email alerts for unauthorized hardware
- List of approved nonstandard software
- A risk management tool to track operational risks
- A disciplined approach for managing changes to systems and reviewing security impacts
- Security plans based on risk that identify minimum baseline controls selected and implemented for internal systems
- Independent assessments of controls
- A process for tracking information security weaknesses and their status
- Continuous communication related to information system security risks among IT staff and senior management
- A process for authorizing information systems based on acceptable risks

Protect

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

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

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

Protect: Configuration Management

According to NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Configuration Management comprises, "a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems..." A baseline configuration is, "a documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures."

We determined FCA's configuration management program is effective based on the configuration management metrics developed by DHS and related testing we performed during this evaluation. The overall maturity rating level for FCA's configuration management program is **Level 4, Managed and Measurable.**

The configuration management program includes the following attributes:

- Information resource management planning process that guides enterprise wide IT asset management and investment control
- Change Control Board[2] that reviews each proposed change for adverse security risks and configuration impacts
- Standard baseline configuration for workstations and servers
- Automated alerts that warn of unauthorized hardware on the network
- Routine scanning and remediation of system vulnerabilities
- Automated process for identification and installation of patches
- A process for approving deviations from the standard configuration

[2]Change Control Board voting members are the CIO, all OIT Associate Directors, all OIT Team Supervisors, and the CISO.

Protect: Identity and Access Management

Identity Management and Access Control is defined in the Cybersecurity Framework. "Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions."

The overall maturity level for FCA's identity and access management program is **Level 3, Consistently Implemented.** We determined FCA's identity and access management program is not effective based on the metrics developed by DHS and related testing we performed during this evaluation. FCA is in the process of automating additional controls for identity access management and strengthening its use of multi-factor authentication which will help it progress to the Managed and Measurable level.

The identity and access management program includes the following attributes:

- Certification that employees and contractors have read the Agency's policy on information security
- System access based on least privilege
- Automated mechanisms for account management
- Alerts for suspicious account activity
- Alerts for unauthorized devices connected to network
- Multi-factor authentication for most users
- Continuous monitoring of privileged accounts

OIT employs the concept of least privilege, which provides the least amount of access required to perform business functions. OIT has a control for reviewing network share access annually, and OIT performed an annual review of network shares in the past. However, the annual review of network shares was not completed in FY 2018.

Agreed-upon Action:

1. OIT needs to ensure network share access is reviewed annually.

Protect: Data Protection and Privacy

OMB develops privacy policy and oversees implementation by Federal agencies. Over the past few years, OMB has significantly increased privacy guidance issued in the form of memoranda and circulars.

OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(c)(2) (July 28, 2016), requires agencies to:

> "Develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program."

OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(e) (July 28, 2016), defines the Senior Agency Official for Privacy's (SAOP) responsibilities:

> "The SAOP has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to manage privacy risks, develop and evaluate privacy policy, and ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems."

The overall maturity level for FCA's data protection and privacy program is **Level 1, Ad Hoc**. We determined FCA's data protection and privacy program is not effective based on the metrics developed by DHS and related testing we performed during this evaluation. Currently, FCA is limited to performing minimal privacy activities, which are a collateral duty of existing staff in the Office of General Counsel (OGC) and OIT.

Protect: Data Protection and Privacy

The data protection and privacy program includes the following attributes:

- A proposed project to develop a privacy program
- The CIO was designated the senior Agency official responsible for information privacy issues and a senior attorney in OGC was designated the Privacy Act Officer
- A breach response plan that includes policies and procedures for data breach reporting, assessment, and notification of affected parties due to a data breach, as well as identifies data breach response team members and incident management team members
- Full disk encryption to encrypt laptop hard drives
- Enhanced network defenses that monitor network traffic and protect against malicious sites and traffic
- Requirement for data on a Universal Serial Bus (USB) drive to be encrypted
- No data breaches requiring reporting during the past year
- A Privacy Act course developed by OGC for OIT

OIT provides employees and contractors with annual information security and privacy awareness training that addresses the following:

- Personally identifiable information (PII) and sensitive information must be safeguarded whether paper or electronic
- PII and sensitive information in emails and attachments sent externally must be encrypted
- Encrypted portable devices are issued upon request
- Agency sensitive information should not be sent or saved on non-FCA equipment or internet accounts

Protect: Data Protection and Privacy

Although FCA took some steps to develop a data protection and privacy program, we identified the following areas that need improvement:

- FCA has not developed a privacy program with policies and procedures that comply with OMB A-130 and A-108.
- OIT documented policies and procedures for some controls to protect PII and sensitive data. However, FCA needs to ensure policies and procedures are based on technologies currently used at FCA and address all PII and sensitive data.
- FCA has not defined policies and procedures related to data exfiltration or implemented a data loss prevention capability.

Agreed-upon Actions:

2. OIT needs to develop and disseminate a privacy program with related plans, policies, and procedures for the protection of PII and other sensitive data collected, used, maintained, shared, and disposed of by information systems. The resources, roles, and responsibilities needed to implement the privacy program must be determined.
3. OIT needs to develop and communicate policies and procedures that identify the inventory of PII and other sensitive data collected, used, and maintained that require increased protection.
4. OIT needs to formalize policies and procedures for:
    - Encryption of data at rest
    - Encryption of data in transit
    - Limitation of transfer to removable media
    - Sanitization of digital media prior to disposal or reuse
5. OIT needs to develop policies and procedures related to preventing data exfiltration.

Protect: Security and Privacy Training

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, states, "A successful IT security program consists of: 1) developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policies and procedures; and 3) establishing processes for monitoring and reviewing the program."

We determined FCA's security training program is effective based on the metrics developed by DHS and related testing we performed during this evaluation. The overall maturity level for FCA's security training program is **Level 4, Managed and Measurable,** which is defined as effective.

The security training program includes the following attributes:

- Training materials for annual security and privacy awareness training that contained content relative to the Agency
- Training materials for new employee and contractor orientation
- Tracking security and privacy awareness training to ensure all information system users attended security and privacy awareness training
- Measuring the effectiveness of its security and privacy awareness and training program through phishing exercises
- Additional counseling for users that repeatedly visit suspicious websites or click on phishing emails
- Prohibition from accessing personal email on agency laptops
- Specialized training for individuals with significant security responsibilities
- Two Certified Information System Security Professionals (CISSP)

Detect

The information security function area for Detect includes the following domain:

- ISCM

We evaluated the domain, Detect, using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for **Level 3, Consistently Implemented**. The following pages provide a summary of the attributes in the ISCM domain.

Detect: Information Security Continuous Monitoring

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, states, "ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

We determined FCA's ISCM is not effective based on the ISCM management metrics developed by DHS and related testing we performed during this evaluation. The overall maturity level for FCA's ISCM program is **Level 3, Consistently Implemented**. Within the context of DHS's maturity model, Managed and Measurable is considered an effective level of security.

FCA's ISCM program includes the following attributes:

- ISCM strategy that provides visibility into IT assets
- Awareness of vulnerabilities and threats
- Security alerts
- Weekly security briefings that include a discussion of the top 10 risks, vulnerabilities, and significant items observed during monitoring
- Annual penetration tests
- Security control assessments performed by independent contractors
- Process for tracking weaknesses identified during audits, inspections, penetration tests, and security control assessments

For FCA's ISCM program to mature to Managed and Measurable and be considered effective, FCA needs to transition to ongoing security control assessments and authorizations. OMB M-14-03, Enhancing the Security of Federal Information and Information Systems, states, "Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems." This includes the ongoing authorization of common controls inherited by organization information systems. OMB M-14-03 further states, "The complete transition

Detect: Information Security Continuous Monitoring

to ongoing authorization should be implemented in accordance with the specific transition criteria established by agencies." OIT has a process for performing security control assessments and granting system authorizations over a three-year cycle for existing systems. However, OIT has not transitioned to ongoing assessments and authorizations. FCA plans to define a process for ongoing authorizations and security control assessments during FY 2019. OIT's goal is to implement an ongoing authorization process with ongoing control assessments and monitoring after the next set of reauthorizations in FYs 2019 and 2020.

Additionally, FCA needs to develop qualitative and quantitative performance measures on the effectiveness of its ISCM program.

Respond

The information security function area for Respond includes the following domain:

- Incident Response

We evaluated the domain, Respond, using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for **Level 3, Consistently Implemented**. The next page provides a summary of the attributes in the Incident Response domain.

Respond: Incident Response

NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, states, "Incident response is the process of detecting and analyzing incidents and limiting the incident's effect." Major phases in the incident response process include:

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activity

The overall maturity level for FCA's incident response program is **Level 3, Consistently Implemented**. We determined FCA's incident response program is not effective based on the metrics developed by DHS and related testing we performed during this evaluation. To mature to the Managed and Measurable level, FCA needs to develop qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.

The most common incidents at FCA are potential viruses, lost identification cards, and lost iPhones. From October 1, 2017, to June 30, 2018, there were no laptops requiring a rebuild from malware and all reported lost iPhones were recovered.

The incident response program includes the following attributes:

- 24-hour Helpline available to employees needing incident assistance
- Requirement that Agency staff immediately report any IT equipment, laptop, smartphone, tablet, encrypted USB drive, identification card, PII, or sensitive information that is suspected to be missing, lost, or stolen
- Threat alert log for tracking potential incidents
- Collaboration and reporting of security incidents to DHS
- Variety of tools used for incident detection, analysis, and prioritization

Recover

The information security function area for Recover includes the following domain:

- Contingency Planning

We evaluated the domain, Recover, using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for **Level 4, Managed and Measurable,** which is defined as effective. The following page provides a summary of the attributes in the Recover Management domain.

Recover: Contingency Planning

According to NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, "Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods."

We determined FCA's contingency planning program is effective based on the metrics developed by DHS and related testing we performed during this evaluation. The overall maturity level for FCA's contingency planning program is **Level 4, Managed and Measurable**.

The contingency planning program includes the following attributes:

- Continuity of Operations Program that provides a strategy to ensure continuity of essential Agency functions during emergency conditions
- Disaster Recovery Plan that provides guidance on the process needed to immediately respond to disasters or major incidents impacting the Agency's IT services
- Identification of mission essential functions
- Alternate recovery site to facilitate continuity of mission essential functions
- Participation by senior executives and IT specialists during periodic continuity exercises
- Self-evaluation of strengths and weaknesses following an annual continuity exercise
- Information system backup strategy that includes alternate storage facilities

Appendix A: Objectives, Scope, and Methodology

The objective of this evaluation is to conduct an independent evaluation of FCA's information security program using the metrics identified by DHS to determine the effectiveness of the information security program and practices.

The scope of this evaluation covers FCA's Agency-owned and contractor-operated information systems of record as of September 30, 2018. FCA is a single program Agency with 15 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 Federal Information Processing Standards.

In performing this evaluation, we performed the following steps:

- Identified and reviewed Agency policies and procedures related to information security and privacy;
- Built on our understanding from past FISMA evaluations;
- Conducted interviews with the CIO, Chief Information Security Officer (CISO), Associate Director Technology Division, several Information Technology Specialists, and contractors;
- 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, 2018, and did not include a test of all information security controls.

The evaluation was performed at FCA Headquarters in McLean, Virginia, from August 2018 through October 2018.

Observations and results were shared with key IT personnel throughout the evaluation. On October 24, 2018, the CIO and senior evaluator discussed FCA's information security and privacy program and recommendations made during this evaluation. On October 26, 2018, the CIO, CISO, Associate Director Technology Division, IT Specialist, and OIG discussed the draft CyberScope report and recommendations.

This evaluation was performed in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*.

FARM CREDIT ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

Report Fraud, Waste, Abuse, Mismanagement

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