Farm Credit Administration

Office of Inspector General

Evaluation Report

2024 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

E-24-01

July 26, 2024

FCAOIG

Farm Credit Administration
Office of Inspector General

FCA OIG
Farm Credit Administration
Office of Inspector General

July 26, 2024

The Honorable Vincent G. Logan, Board Chairman and Chief Executive Officer
The Honorable Jeffery S. Hall, Board Member
The Honorable Glen R. Smith, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, VA 22102-5090

Dear Chairman Logan and Board Members Hall and Smith:

The Federal Information Security Modernization Act of 2014 (FISMA) requires the Inspector General of each agency to annually conduct an independent evaluation of the agency's information security program. The Office of Inspector General conducted an evaluation in accordance with the Fiscal Year 2024 Inspector General FISMA Reporting Metrics.

The attached evaluation report summarizes the results of the evaluation. We concluded that the Farm Credit Administration's (FCA) information security program is effective based on our analysis of the core and supplemental metrics under the scoring methodology. FCA continues to improve the information security program and closed all previous FISMA recommendations. However, we made three recommendations to improve certain areas. The Agency agreed with, and provided corrective actions, for all recommendations in the report.

The FISMA report contains information which, if disclosed, may adversely affect information security. Therefore, portions of this report containing sensitive information are redacted before publishing the report on our website.

We appreciate the courtesies and professionalism extended by FCA to our staff during the evaluation, especially the Office of Information Technology. If you have any questions, we would be pleased to meet with you at your convenience.

Respectfully,

Sonya K. Cerne
Assistant Inspector General for Audits, Inspections, and Evaluations

EXECUTIVE SUMMARY

2024 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

Report No. E-24-01 July 26, 2024

Objective

The objective of this evaluation was to determine the effectiveness of FCA's information security program for fiscal year 2024.

Recommendations

We made three recommendations in the report to address improvements needed in information security continuous monitoring and [redacted]

Agency Response

Management agreed with, and provided responsive corrective actions for, all recommendations made in the report.

Why We Did This Evaluation

The Federal Information Security Modernization Act of 2014 (FISMA) requires offices of inspector general to perform an annual independent evaluation of their agency's information security program and practices to determine the effectiveness of the program and practices. The Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency, in consultation with other stakeholders, developed the Fiscal Year 2023-2024 Inspector General (IG) FISMA Reporting Metrics. According to the IG FISMA metrics, one of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementing the Administration's priorities and best practices. This evaluation of the Farm Credit Administration (FCA) covers the period from July 1, 2023, to June 30, 2024.

What We Found

The evaluation found that FCA has an information security program that continues to mature. FCA's information security program is ranked effective based on the analysis of 20 core metrics and 17 supplemental metrics under the scoring methodology. The table below summarizes the results from CyberScope's scoring.

Fiscal Year 2024 Ratings by Function and Domain

Function	Domain	Rating Assigned in CyberScope
Identify	Risk Management	Managed and Measurable
Identify	Supply Chain Risk Management	Consistently Implemented
Protect	Configuration Management	Managed and Measurable
Protect	Identity and Access Management	Managed and Measurable
Protect	Data Protection and Privacy	Managed and Measurable
Protect	Security Training	Managed and Measurable
Detect	Information Security Continuous Monitoring	Defined
Respond	Incident Response	Managed and Measurable
Recover	Contingency Planning	Consistently Implemented

Portions of this report have been redacted to protect information that, if disclosed, may adversely affect information security.

TABLE OF CONTENTS

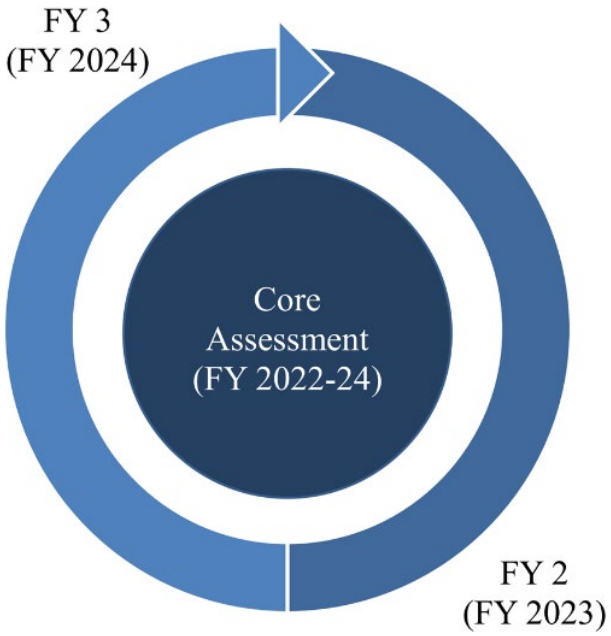
BACKGROUND

The Farm Credit Administration (FCA or Agency) is an independent federal agency responsible for regulating and supervising the Farm Credit System (System). The Agency is responsible for ensuring that all System institutions are safe, sound, and dependable sources of credit and related services for all creditworthy and eligible persons in agriculture and rural America. In order to successfully achieve this mission, FCA needs to have an effective information security program that protects the Agency and its data and complies with security requirements.

The Federal Information Security Modernization Act of 2014 (FISMA), which reformed the Federal Information Security Management Act of 2002, was enacted on December 18, 2014. FISMA outlines the information security management requirements for agencies, including an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA requires the annual evaluation to be performed by the agency's Office of Inspector General (OIG) or by an independent external auditor, as determined by the Inspector General (IG) of the agency.

IG FISMA Reporting Metrics

The Office of Management and Budget (OMB), the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders worked collaboratively to develop the Fiscal Year (FY) 2023-2024 IG FISMA Reporting Metrics. These metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, provides reporting guidance and deadlines for the IG annual metrics in the Department of Homeland Security's (DHS) CyberScope application.



FY 2023 was the first year of the multi-year cycle. The metrics for FY 2024 continue the cycle with a focus on 20 "core" metrics and 17 "supplemental" metrics. The core IG metrics were chosen based on their alignment with Executive Order 14028, *Improving the Nation's*

Cybersecurity, as well as OMB guidance to agencies to improve federal cybersecurity. The following graphic further explains core and supplemental metrics.

Core Metrics

Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

Supplemental Metrics

Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

Cybersecurity Framework

The IG FISMA Reporting Metrics are aligned with the five function areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): identify, protect, detect, respond, and recover. The metrics state that, "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 controls to address those risks."

NIST released the Cybersecurity Framework 2.0 in February 2024, which changes the structure of the framework.[1] Due to the timing and scope, the Cybersecurity Framework 2.0 implementation is not part of the review for this year.

Cybersecurity Framework 2.0

The FY 2023-2024 IG FISMA Reporting Metrics emphasize the importance of cybersecurity across federal agencies. OMB,

[1] The Cybersecurity Framework 2.0 revolves around new core Functions: Govern, Identify, Protect, Detect, Respond, and Recover. NIST explains in the framework that each Function is named after a verb that summarizes its contents. Each Function is divided into Categories, which are related cybersecurity outcomes that collectively comprise the Function. Subcategories further divide each Category into more specific outcomes of technical and management activities. The Subcategories are not exhaustive, but they describe detailed outcomes that support each Category (***The NIST Cybersecurity Framework (CSF) 2.0***).

CIGIE, and other stakeholders developed the metrics using the NIST Cybersecurity Framework's five information security functions (before the 2.0 update) with nine associated domains:

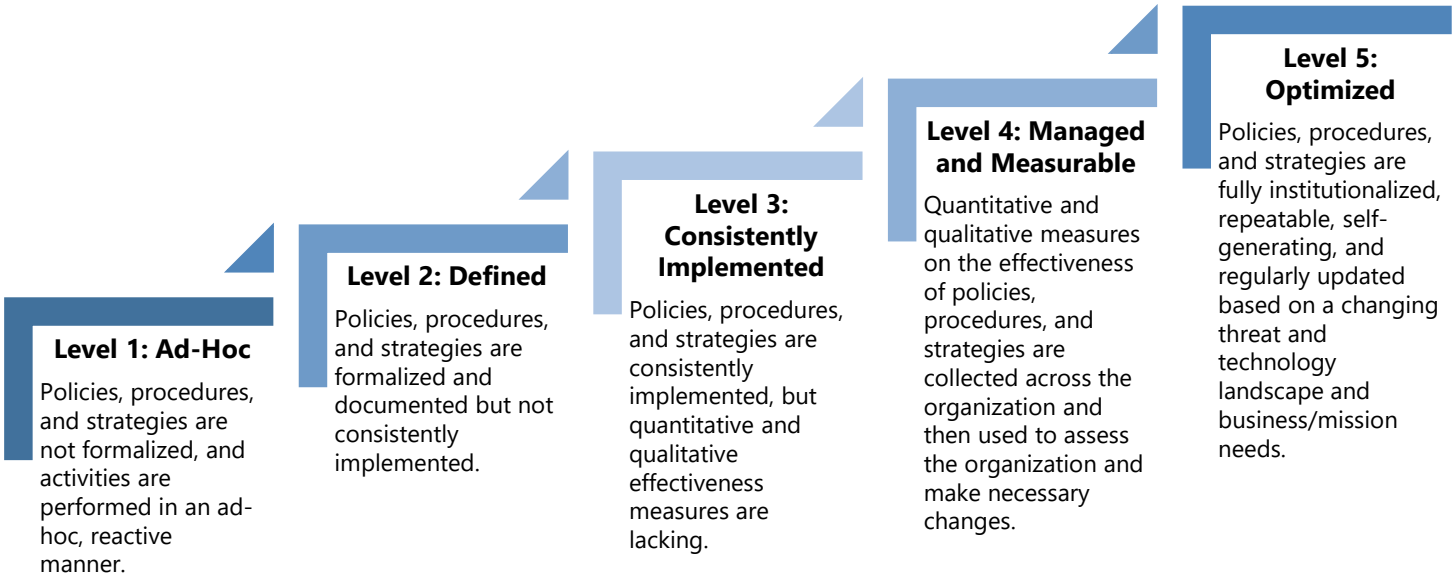
FY 2023-2024 IG FISMA Reporting Metrics by Function and Domain

Function	Domain
Identify	**Risk Management**
Identify	**Supply Chain Risk Management**
Protect	**Configuration Management**
Protect	**Identity and Access Management**
Protect	**Data Protection and Privacy**
Protect	**Security Training**
Detect	**Information Security Continuous Monitoring**
Respond	**Incident Response**
Recover	**Contingency Planning**

Ratings in FY 2023 and FY 2024 focus on a calculated average approach, wherein the average of the metrics will be used by IGs to determine the effectiveness of each domain and function. This is a change in scoring methodology from the previous reviews, which were based on the mode.

Maturity Models

According to the IG FISMA Reporting Metrics, the effectiveness of an information security program is determined based on the ratings earned on a maturity model spectrum, which identifies whether an agency has developed policies and procedures, implemented documented processes, and established methods to improve over time. The FISMA maturity model summarizes the status of agencies' information security programs on a five-level scale (Level 1 to Level 5). The maturity model spectrum is divided into five levels outlined below:



According to the FY 2023-2024 IG FISMA Reporting Metrics, a Level 4, Managed and Measurable, or above, means the information security program is operating at an effective level of security. Generally, a Level 4 maturity level is defined as formalized, documented, and consistently implemented policies, procedures, and strategies with quantitative and qualitative performance measures on the effectiveness of policies, procedures, and strategies collected across the organization and assessed to make necessary changes.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this evaluation was to determine the effectiveness of FCA's information security program for FY 2024. We determined the effectiveness of FCA's information security program and practices using the IG FISMA metrics. In reporting the CyberScope results, we relied on the guidance set forth in OMB Memorandum M-24-04.

Scope

The scope of the evaluation was limited to FCA's implementation of FISMA requirements for FY 2024 (July 1, 2023, through June 30, 2024). This included an assessment of the effectiveness of FCA's enterprise-wide information security policies, procedures, and practices, and a review of information security policies, procedures, and practices for FCA's information systems, as applicable. The evaluation was conducted at FCA's headquarters in McLean, Virginia from April through July 2024.

Methodology

The OIG took the following steps to accomplish the objective:

- Identified and reviewed applicable laws, regulations, guidance, and other background information applicable to the objective.
- Identified and reviewed applicable internal FCA policies and procedures.
- Reviewed prior FCA OIG and other external reviews related to the objective.
- Conducted interviews and walkthroughs with certain Office of Information Technology (OIT) staff.
- Assessed the effectiveness of FCA's efforts to secure its information systems. This included an assessment of each function and domain, as specified in the IG FISMA Reporting Metrics for FY 2024:
    - Identify (Risk Management)
    - Identify (Supply Chain Risk Management)
    - Protect (Configuration Management)
    - Protect (Identity and Access Management)
    - Protect (Data Protection and Privacy)
    - Protect (Security Training)
    - Detect (Information Security Continuous Monitoring)
    - Respond (Incident Response)
    - Recover (Contingency Planning)
- Performed testing to accomplish the objective. This testing included sampling systems, software, and other items to address applicable metrics. These samples were judgmentally selected based on use, risk, and support needed to assess the maturity level for metrics. Therefore, we cannot project the samples to the population of all information security elements.

Quality Standards for Inspection and Evaluation

This evaluation was performed in accordance with CIGIE's Quality Standards for Inspection and Evaluation. These standards require that we plan and perform the evaluation to obtain sufficient and appropriate evidence that provides a reasonable basis for our findings, conclusions, and recommendations. We assessed internal controls and compliance with laws and regulations to the extent necessary to satisfy the objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our evaluation. We assessed the information and data collected during the evaluation and determined it was sufficiently reliable and valid for use in meeting the evaluation objective. We assessed the risk of fraud related to our evaluation objective while evaluating evidence and had no matters come to our attention indicating fraud or illegal acts were occurring. Overall, we believe the evidence obtained is appropriate and sufficient to provide a reasonable basis for our findings and conclusions based on the evaluation objective.

EVALUATION RESULTS

Based on the IG FISMA metric requirements, the ratings in CyberScope, and the work performed as part of this evaluation, FCA has implemented an effective information security program for FY 2024. FCA continued to improve its information security program. FCA also made progress in implementing the recommendations resulting from previous FISMA reviews and closed all open recommendations by November 2023.

Additional elements of the information security program include:

- Updated information security policies and procedures,
- Corrective action processes for significant information security weaknesses,
- Use of a Change Control Board,
- Risk management tools and practices,
- Vulnerability and security control assessments,
- Alerts for suspicious activity and devices,
- Weekly security meetings, and
- Continuous Diagnostic and Monitoring tools.

FCA OIG reported the results of the evaluation in DHS's CyberScope application. The table below summarizes the results based on CyberScope's scoring. Each function and domain are discussed in more detail in the subsequent sections of this report.

FY 2024 CyberScope Ratings by Function and Domain

Function	Domain	Rating Assigned in CyberScope
Identify	Risk Management	Level 4: Managed and Measurable
Identify	Supply Chain Risk Management	Level 3: Consistently Implemented
Protect	Configuration Management	Level 4: Managed and Measurable
Protect	Identity and Access Management	Level 4: Managed and Measurable
Protect	Data Protection and Privacy	Level 4: Managed and Measurable
Protect	Security Training	Level 4: Managed and Measurable
Detect	Information Security Continuous Monitoring	Level 2: Defined
Respond	Incident Response	Level 4: Managed and Measurable
Recover	Contingency Planning	Level 3: Consistently Implemented

Identify

Level 1
Ad-hoc

Level 2
Defined

Level 3
Consistently Implemented

Level 4
Managed and Measurable

Level 5
Optimized

The Identify function supports an understanding of the business context, the resources that support critical functions, and the related cybersecurity risks that enable an entity to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The Identify function includes the Risk Management and Supply Chain Risk Management domains.

We evaluated the domains in the Identify function using the FISMA guidance. Based on the scoring methodology, FCA met the criteria for Level 4, **Managed and Measurable**.

Risk Management

NIST defines Risk Management as the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

The overall maturity level for FCA's Risk Management program is **Managed and Measurable**. We determined FCA's Risk Management program is effective based on the metrics and related testing performed during this evaluation.

FCA's current Risk Management program includes the following attributes:

- A current system inventory and categorization of all major systems,
- The use of a Change Control Board to track changes in the environment,
- A risk management tool for tracking cybersecurity risks,
- Security controls that identify minimum baseline controls selected and implemented for internal information systems,
- A process for tracking identified information security weaknesses through plans of action and milestones,
- Regular and timely internal office communications related to security risks,
- Communication of risks in a timely and consistent manner with senior management, and
- A process for authorizing information systems based on acceptable risks.

Supply Chain Risk Management

Supply Chain Risk Management is the systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures.

The overall maturity level for FCA's Supply Chain Risk Management program is **Consistently Implemented**. We determined FCA's Supply Chain Risk Management program is not effective based on the metrics and related testing performed during this evaluation.

FCA's current Supply Chain Risk Management program includes the following attributes:

- A documented process for change management,
- Updated policies and procedures,
- A Change Control Board that reviews proposed changes for adverse security risks, and
- Supply chain risks that have been incorporated into risk management processes.

FCA has defined and communicated Supply Chain Risk Management policies and procedures and made improvements in this domain. However, FCA has not [redacted] Because the Agency continues to develop supply chain risks and tolerances and update policies and procedures in accordance with NIST Special Publication (SP) 800-53, Revision 5, we did not make a recommendation in this area.

Protect

The Protect function seeks to develop and implement safeguards to support the ability to limit or contain the impact of a potential information security event. The Protect function includes the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains.

We evaluated the domains in the Protect function using the FISMA guidance. Based on the scoring methodology, FCA met the criteria for Level 4, **Managed and Measurable**.

Level 1 Ad-hoc
Level 2 Defined
Level 3 Consistently Implemented
Level 4 Managed and Measurable
Level 5 Optimized

Configuration Management

According to NIST, configuration management comprises, "a collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle." A baseline configuration is, "a set of specifications for a system, or 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."

The overall maturity level for FCA's Configuration Management program is **Managed and Measurable**. We determined FCA's Configuration Management program is effective based on the metrics and related testing performed during this evaluation.

The Configuration Management program includes the following attributes:

- A planning process that guides enterprise-wide information technology asset management and investment control,
- A Change Control Board that reviews proposed changes for adverse security risks and configuration impacts,
- Automated monitoring and alerts that detect potential concerns on the Agency network,
- Routine scanning and remediation of system vulnerabilities, and
- Automated processes for identification and installation of patches.

Identity and Access Management

Effective access control processes are critical to prevent unauthorized system access, whether by internal employees or external attackers, that could endanger the confidentiality, integrity, and availability of FCA systems. Proper identity and access management help ensure that only approved and authorized personnel have access to FCA information.

The overall maturity level for FCA's Identity and Access Management program is **Managed and Measurable**. We determined FCA's Identity and Access Management program is effective based on the metrics and related testing performed during this evaluation.

FCA's Identity and Access Management program includes the following attributes:

- Risk designations and appropriate personnel screening,
- Automated mechanisms for account management,
- Multi-factor authentication for all privileged and non-privileged users, and
- Continuous monitoring of privileged accounts.

Data Protection and Privacy

Data Protection and Privacy can be summarized as preventing the unwanted release of sensitive information and responding to any instances where information is found to be inadvertently shared.

The overall maturity level for FCA's Data Protection and Privacy program is **Managed and Measurable**. We determined FCA's Data Protection and Privacy program is effective based on the metrics and related testing performed during this evaluation.

FCA's Data Protection and Privacy program includes the following attributes:

- A breach response plan that includes policies and procedures for data breach reporting and assessment, notification to affected parties, and team members for data breach response and incident management,
- An annual information security and privacy awareness training program,
- Phishing campaign exercises to test employees' knowledge and training,
- Policies and procedures for data at rest, data in transit, media sanitization, and limitation of removable media, and
- The implementation of data loss prevention tools.

Security Training

Security training helps to ensure that personnel at all levels understand their information security responsibilities and how to properly use and protect the information and the resources entrusted to them. Therefore, a well-defined security training process must include continual training of the workforce on the security policy, and responsibilities for all users under the security policy, to ensure the protection of FCA assets and information.

The overall maturity level for FCA's Security Training program is **Managed and Measurable**. We determined FCA's Security Training program is effective based on the metrics and related testing performed during this evaluation.

FCA's Security Training program includes the following attributes:

- Annual IT security awareness training that contained content relative to the Agency,
- Role-based security training for FCA managers and supervisors,
- Security awareness training metrics that are used to ensure information system users completed and understood the training, and
- Phishing exercises that educate employees on how to identify potential phishing threats.

Detect

Level 1
Ad-hoc

Level 2
Defined

Level 3
Consistently Implemented

Level 4
Managed and Measurable

Level 5
Optimized

The Detect function enables timely discovery of an information security event and supports successful incident response and recovery activities. The Detect function comprises one domain, Information Security Continuous Monitoring.

We evaluated the domain in the Detect function using the FISMA guidance. Based on the scoring methodology, FCA met the criteria for Level 2, **Defined**.

Information Security Continuous Monitoring

Information Security Continuous Monitoring enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An Information Security Continuous Monitoring program helps to ensure that deployed security controls continue to be effective and that operations remain within stated organizational risk tolerances. Ongoing monitoring of information security across an organization begins with defining a comprehensive information security continuous monitoring strategy encompassing technology, processes, procedures, operating environments, and people.

The overall maturity level for FCA's Information Security Continuous Monitoring program is **Defined**. We determined FCA's Information Security Continuous Monitoring program is not effective based on the metrics and related testing performed during this evaluation.

FCA's Information Security Continuous Monitoring program includes the following attributes:

- A strategy that provides visibility into information technology assets,
- An awareness of vulnerabilities and threats,
- Weekly security briefings that include a discussion of the top risks, vulnerabilities, and significant items observed during monitoring,
- Annual penetration tests,
- Security control assessments performed by independent contractors, and
- A process for tracking weaknesses identified during audits, inspections, penetration tests, and security control assessments.

OIT revised its Information Security and Privacy Policy in accordance with NIST SP 800-53, Revision 5, in August 2023, and resolved previous FISMA recommendations related to this area. [redacted]

[redacted]

Recommendation

1. [redacted]

Agency Response
Management agreed with the recommendation and stated they will [redacted] Management estimated the actions would be completed by January 2025.

OIG Response
OIG finds the actions responsive to our recommendation.

Respond

The Respond function supports the ability to act in response to a detected cybersecurity incident and to limit the incident's impact. The Respond function includes the Incident Response domain.

We evaluated the domain in the Respond function using the FISMA guidance. Based on the scoring methodology, FCA met the criteria for Level 4, **Managed and Measurable.**

Incident Response

Incident response is how an Agency detects and analyzes incidents and then limits an incident's effect.

The overall maturity level for FCA's Incident Response program is **Managed and Measurable**. We determined FCA's Incident Response program is effective based on the metrics and related testing performed during this evaluation.

FCA's Incident Response program includes the following attributes:

- A helpline available to employees needing incident assistance,

Level 1 Ad-hoc
Level 2 Defined
Level 3 Consistently Implemented
Level 4 Managed and Measurable
Level 5 Optimized

[2] [redacted]

- A requirement that Agency staff immediately report to the Helpline any suspected security incidents,
- Risk assessment for all incidents,
- A threat alert site for tracking potential incidents,
- Reporting of security incidents to DHS,
- Notifications of security incidents to the OIG, and
- A variety of tools used for incident detection, analysis, and prioritization.

Recover

Level 1
Ad-hoc

Level 2
Defined

Level 3
Consistently Implemented

Level 4
Managed and Measurable

Level 5
Optimized

The Recover function seeks to reduce the negative impact from a cybersecurity incident by maintaining plans to restore impaired capabilities or services. The Recover function includes the Contingency Planning domain.

We evaluated the domain using the FISMA guidance. Based on the scoring methodology, FCA met the criteria for Level 3, **Consistently Implemented**.

Contingency Planning

According to NIST, 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.

The overall maturity level for FCA's Contingency Planning program is **Consistently Implemented**. We determined FCA's Contingency Planning program is not effective based on the metrics and related testing performed during this evaluation.

FCA's Contingency Planning program includes the following attributes:

- A Continuity of Operations Program that provides a strategy to ensure continuity of essential Agency functions during emergency conditions,
- A Disaster Recovery Plan that provides guidance on the process needed to immediately respond to disasters or major incidents impacting the Agency's IT services,
- Continuity testing plans and procedures to validate recovery capabilities,
- System-specific information system contingency plans and business impact analyses,
- An information system backup strategy that includes alternate storage facilities,
- Identification of mission essential functions, and

- An alternate recovery site to facilitate continuity of mission essential functions.

During the review, we identified weaknesses in FCA's Contingency Planning program. [redacted] The role of the Disaster Recovery Plan is to provide the essential guidance on the process needed to respond immediately to events arising from a disaster or major incident that involves a disruption to the network and its services and minimize the effects a disaster or major incident will have on continuing operations.

[redacted] Contingency planning generally includes information system contingency planning, continuity of operations planning, and disaster recovery planning with wide-ranging impacts across the Agency. Because contingency planning impacts stakeholders in multiple offices, additional communication is needed to ensure those with responsibilities outlined in planning, testing, and exercises understand requirements set forth in continuity plans. Regular testing and maintenance activities ensure contingency plans are current and effective.

Recommendations

2. [redacted]

3. [redacted]

Agency Response
Management agreed with the recommendations and stated they will [redacted] Management estimated the actions would be completed by December 2024.

OIG Response
OIG finds the actions responsive to our recommendations.

Management waived an exit conference and did not provide formal comments to the report.

ACRONYMS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
FCA or Agency	Farm Credit Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
SP	Special Publication

FCA OIG

Farm Credit Administration
Office of Inspector General

REPORT FRAUD, WASTE, ABUSE, & MISMANAGEMENT:

Fraud, waste, abuse, and mismanagement in government concerns everyone: Office of Inspector General staff, FCA employees, Congress, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to FCA programs and operations. You can report allegations to us in several ways:

Online:	**https://apps.fca.gov/oigcomplaint**
Phone:	**(800) 437-7322 (Toll-Free)** **(703) 883-4316**
Email:	**fca-ig-hotline@rcn.com**
Mail:	**1501 Farm Credit Drive** **McLean, VA 22102-5090**

To learn more about reporting wrongdoing to the OIG, please visit our website at https://www.fca.gov/about/inspector-general.