Farm Credit Administration

Office of Inspector General

Evaluation Report

2025 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

E-25-01

July 23, 2025

FCAOIG

Farm Credit Administration
Office of Inspector General

FCA OIG

Farm Credit Administration
Office of Inspector General

July 23, 2025

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

Dear Chairman Hall and Board Member Smith:

The Federal Information Security Modernization Act of 2014 (FISMA), as amended, 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 2025 Inspector General FISMA Reporting Metrics.

The attached 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 four 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

2025 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

Report No. E 25 01 July 23, 2025

Objective

The objective of this evaluation was to determine the effectiveness of FCA's information security program for fiscal year 2025.

Recommendations

We made four recommendations in the report to improve cybersecurity governance, risk and asset management, and incident response.

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), as amended, requires offices of inspector general to perform an annual independent evaluation of the effectiveness of their agency's information security 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 2025 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 objectives 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, 2024, to June 30, 2025.

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 25 metrics under the scoring methodology. The table below summarizes the results from CyberScope's scoring.

Fiscal Year 2025 Ratings by Function and Domain

Function	Domain	Rating Assigned in CyberScope
Govern	Cybersecurity Governance	Consistently Implemented
Govern	Cybersecurity Supply Chain Risk Management	Managed and Measurable
Identify	Risk and Asset 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	Managed and Measurable
Respond	Incident Response	Consistently Implemented
Recover	Contingency Planning	Managed and Measurable

TABLE OF CONTENTS

BACKGROUND

The Farm Credit Administration (FCA or Agency) is a federal agency responsible for regulating and supervising the Farm Credit System. The Agency is responsible for ensuring that all Farm Credit 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, as amended, 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) 2025 IG FISMA Reporting Metrics. OMB Memorandum M-25-04, *Fiscal Year 2025 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.

The FY 2025 IG FISMA Reporting metrics no longer include a multi-year approach; however, the metrics continue to focus on "core" metrics and "supplemental" metrics. 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 not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

Cybersecurity Framework

The FY 2025 IG FISMA Reporting Metrics are now aligned with the six function areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (Cybersecurity Framework 2.0): govern, identify, protect, detect, respond, and recover. NIST released the Cybersecurity Framework 2.0 in February 2024, which changed the structure of the previous cyber security framework. The Cybersecurity Framework 2.0 revolves around a new Govern function.

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.

Cybersecurity Framework 2.0

The FY 2025 IG FISMA Reporting Metrics emphasize the importance of cybersecurity across federal agencies. OMB, CIGIE, and other stakeholders developed the metrics using the Cybersecurity Framework 2.0 information security functions with ten associated domains:

FY 2025 IG FISMA Reporting Metrics Functions and Domains

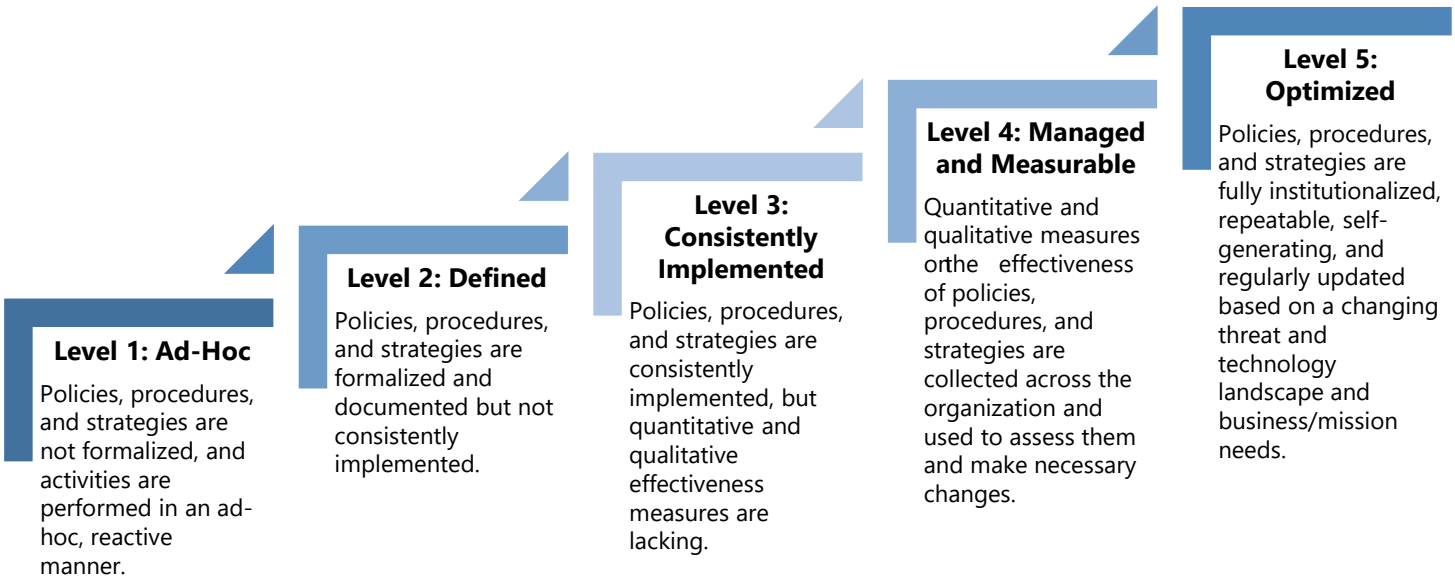
Function	Domain
Govern	**Cybersecurity Governance**
Govern	**Cybersecurity Supply Chain Risk Management**
Identify	**Risk and Asset Management**
Protect	**Configuration Management**
Protect	**Identity and Access Management**
Protect	**Data Protection and Privacy**
Protect	**Security Training**

Detect	**Information Security Continuous Monitoring**
Respond	**Incident Response**
Recover	**Contingency Planning**

Ratings for this period continue to focus on a calculated average approach, wherein the average of the metrics is used by IGs to determine the effectiveness of each domain and function.

Maturity Models

According to the FY 2025 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 2025 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 2025. We determined the effectiveness of FCA's information security program and practices using the IG FISMA Reporting Metrics. In reporting the CyberScope results, we relied on the guidance set forth in OMB Memorandum M-25-04.

Scope

The scope of the evaluation was limited to FCA's implementation of FISMA requirements for July 1, 2024 through June 30, 2025. 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 2025.

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 reviews related to the objective.
- Conducted interviews and walkthroughs with certain Office of Information Technology and Office of Agency Services 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 2025:
    - Govern (Cybersecurity Governance)
    - Govern (Cybersecurity Supply Chain Risk Management)
    - Identify (Risk and Asset 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 FY 2025 IG FISMA Reporting Metrics, ratings in CyberScope, and work performed as part of this evaluation, FCA has implemented an effective information security program for FY 2025. 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.

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;
- Investment in new and upgraded technologies and tools;
- Alerts for suspicious activity and devices;
- Weekly security meetings; and
- Continuous Diagnostics and Mitigation 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 2025 CyberScope Ratings by Function and Domain

Function	Domain	Rating Assigned in CyberScope
Govern	Cybersecurity Governance	Level 3: Consistently Implemented
Govern	Cybersecurity Supply Chain Risk Management	Level 4: Managed and Measurable
Identify	Risk and Asset 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 4: Managed and Measurable
Respond	Incident Response	Level 3: Consistently Implemented
Recover	Contingency Planning	Level 4: Managed and Measurable

Govern

The Govern function is new to the IG metrics this year. The Govern function helps address an understanding of organizational context, cybersecurity strategy, cybersecurity supply chain risk management, authorities, policy, and oversight. The Govern function includes the Cybersecurity Governance and Cybersecurity Supply Chain Risk Management domains.

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

Level 1
Ad hoc

Level 2
Defined

Level 3
Consistently Implemented

Level 4
Managed and Measurable

Level 5
Optimized

Cybersecurity Governance

The Cybersecurity and Infrastructure Security Agency defines Cybersecurity Governance as a comprehensive cybersecurity strategy that integrates with organizational operations and prevents the interruption of activities due to cyber threats or attacks.

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

FCA's current Cybersecurity Governance program includes the following attributes:

- A cybersecurity risk management strategy to support operational risk decisions;
- A cybersecurity connection to the enterprise risk management strategy;
- Use of automated tools, dashboards, and metrics to inform governance;
- Cybersecurity duties included in position descriptions; and
- Accountability in implementation of cybersecurity requirements.

During the review, we found that FCA has not [redacted]

While FCA has a robust risk management process, the Agency has not developed [redacted]

Recommendation

1. The Office of Inspector General recommends the Office of Information Technology [redacted]

Agency Response
Management agreed with the recommendation and stated they will [redacted] Management estimated the actions would be completed by January 2026.

OIG Response
OIG finds the actions responsive to our recommendation.

Cybersecurity Supply Chain Risk Management

Cybersecurity Supply Chain Risk Management is a 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 Cybersecurity Supply Chain Risk Management program is **Managed and Measurable**. We determined FCA's Cybersecurity Supply Chain Risk Management program is effective based on the metrics and related testing performed during this evaluation.

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

- Change management operating procedures;
- Supply chain risk management policies and procedures in the information security and privacy policy;
- A Change Control Board that reviews proposed changes for adverse security risks; and
- Supply chain risks incorporated into risk management processes.

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 assets, suppliers and related cybersecurity risks that enables an organization to prioritize its efforts consistent with its risk management strategy and mission needs. The Identify function includes the Risk and Asset Management domain.

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

Risk and Asset 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 and Asset Management program is **Consistently Implemented**. We determined FCA's Risk and Asset Management program is not effective based on the metrics and related testing performed during this evaluation.

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

- A current system inventory and categorization of all major systems;
- Changes to the environment tracked through a Change Control Board;
- A risk management tool for tracking cybersecurity risks;
- Monitoring processes for information systems;
- Regular and timely communications related to information system security risks among information technology staff; and
- A software inventory that includes licenses.

The Continuous Diagnostics and Mitigation (CDM) program is an important tool for risk and asset management for FCA. The CDM program was developed in 2012 to support government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks. Additionally, the program increases visibility into the federal cybersecurity posture and streamlines FISMA reporting through the delivery of cybersecurity tools, integration services, and dashboards through the Cybersecurity and Infrastructure Security Agency. There have been several requirements and directives issued to

agencies outlining responsibilities on asset visibility and endpoint detection and response including, but not limited to:

- **Binding Operational Directive 23-01: *Improving Asset Visibility and Vulnerability Detection of Federal Networks***;
- **Executive Order 14028: *Improving the Nation's Cybersecurity***; and
- **OMB M-22-01: *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response***.

FCA has made great strides in placing Agency assets into the CDM program and continues to improve asset visibility and endpoint detection automation. [redacted]

Another important element of risk and asset management is that assets that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. This year, a new metric focuses on the maturity level for data inventories. [redacted]

Recommendations

To improve the Risk and Asset Management program:

2. The Office of Inspector General recommends the Office of Information Technology [redacted]
3. The Office of Inspector General recommends the Office of Information Technology, in coordination with the Office of Data Analytics and Economics, [redacted]

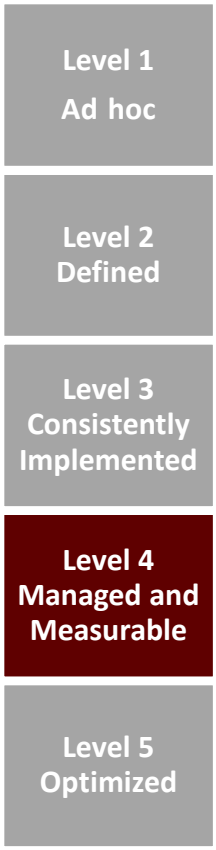
Agency Response
Management agreed with the recommendations and stated they will work with the Cybersecurity and Infrastructure Security Agency [redacted] Management estimated the actions would be completed by March 2026. Management also stated they would [redacted] and estimated these actions would be completed by December 2025.

OIG Response
OIG finds the actions responsive to our recommendations.

Protect

The Protect function seeks to develop and implement safeguards to support the ability to limit or contain the likelihood and 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**.



Configuration Management

According to NIST, 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 throughout the system development life cycle."

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:

- Policies and procedures for configuration management and flaw remediation;
- 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 in preventing 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:

- Automated mechanisms for account management;
- Multi-factor authentication for privileged and non-privileged users; and
- Continuous monitoring of accounts.

Data Protection and Privacy

Data Protection and Privacy can be summarized as preventing the unwanted release of sensitive information.

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:

- Policies and procedures for data at rest, data in transit, media sanitization, and limitation of removable media;
- Encryption to reduce the risk of loss or exposure of Agency data; 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 and privacy trainings that contained content relative to the Agency and related roles;
- Phishing exercises that educate employees on how to identify potential phishing threats; and
- Publication of newsletters and news flashes to FCA employees that help raise and maintain a culture of IT security and privacy awareness at the Agency.

Detect

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

We evaluated the domain in the Detect 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

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. Security controls and organizational risks should be assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

The overall maturity level for FCA's Information Security Continuous Monitoring program is **Managed and Measurable**. We determined FCA's Information Security Continuous Monitoring program is 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;
- 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.

Respond

Level 1
Ad hoc

Level 2
Defined

Level 3
Consistently Implemented

Level 4
Managed and Measurable

Level 5
Optimized

The Respond function supports the ability to contain the effects of cybersecurity incidents. 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 3, **Consistently Implemented**.

Incident Response

Incident response is the process of detecting and analyzing incidents and limiting the incident's effect.

The overall maturity level for FCA's Incident Response program is **Consistently Implemented**. We determined FCA's Incident Response program is not 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;
- A requirement that Agency staff immediately report to the helpline any suspected security incidents;
- Risk assessments for incidents;
- A threat alert site for tracking potential incidents;
- Collaboration on and reporting of security incidents; and
- A variety of tools used for incident detection, analysis, and prioritization.

Due to cybersecurity events across the world, there was a renewed focus on federal agencies' ability to increase visibility before, during, and after a cybersecurity incident. Specifically, event logging (EL) supports the resiliency of systems by enabling network visibility. OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, requires agencies to adhere to a maturity model of EL management across four tiers by certain deadlines as noted in the chart below.

Event Logging Tiers

Event Logging Tiers	Rating	Description	M-21-31 Compliance Achievement dates
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met	
EL1	Basic	Only logging requirements of highest criticality are met	August 2022
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met	February 2023
EL3	Advanced	Logging requirements at all criticality levels are met	August 2023

[redacted]

Recommendation

To improve the Incident Response program:

4. The Office of Inspector General recommends the Office of Information Technology [redacted]

Agency Response

Management agreed with the recommendation and stated they will [redacted] Management estimated the actions would be completed by January 2026.

OIG Response

OIG finds the actions responsive to our recommendation.

Recover

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 4, **Managed and Measurable.**

Level 1
Ad hoc

Level 2
Defined

Level 3
Consistently Implemented

Level 4
Managed and Measurable

Level 5
Optimized

Contingency Planning

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following:

- Restoring information systems using alternate equipment;
- Using alternate processing means for affected processes;
- Recovering information systems operations at an alternate location; and
- Implementing appropriate controls based on the information system's security impact level.

The overall maturity level for FCA's Contingency Planning program is **Managed and Measurable**. We determined FCA's Contingency Planning program is 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 information technology services;
- Continuity testing plans and procedures to validate recovery capabilities; and
- System-specific information system contingency plans and business impact analyses.

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

ACRONYMS

CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
EL	Event Logging
FCA or Agency	Farm Credit Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

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.