Farm Credit Administration

Office of Inspector General

Audit Report

Farm Credit Administration's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2023

A-23-02

July 26, 2023

FCA OIG

Farm Credit Administration
Office of Inspector General

July 26, 2023

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 contracted with the independent public accounting firm Williams, Adley, & Company-DC, LLP (Williams Adley) to conduct an audit for the Fiscal Year 2023 FISMA review. The contract required Williams Adley to follow the Fiscal Year 2023 Inspector General FISMA Reporting Metrics. Williams Adley conducted the audit in accordance with U.S. Generally Accepted Government Auditing Standards.

The attached audit report summarizes the results of Williams Adley's independent audit. Williams Adley concluded that the Farm Credit Administration's (FCA) information security program is effective based on the auditors' analysis of core metrics and supplemental metrics under the Department of Homeland Security's scoring methodology. Williams Adley reported that FCA continues to improve the information security program and did not make any recommendations as part of this year's audit.

In connection with the contract, we monitored the work performed by Williams Adley. Our review, as differentiated from an audit in accordance with U.S. Generally Accepted Government Auditing Standards, was not intended to enable us to express, and we do not express, opinions on or conclusions about the effectiveness of FCA's information security program. Williams Adley is responsible for the attached report and the conclusions expressed therein. However, our review disclosed no instances where Williams Adley did not comply, in all material respects, with U.S. Generally Accepted Government Auditing Standards.

Williams Adley's report contains sensitive information about FCA and potential vulnerabilities that could be used against FCA. Therefore, portions of this report containing sensitive information are redacted before publishing the report on our website.

Respectfully,

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

Enclosure

EXECUTIVE SUMMARY

Farm Credit Administration's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2023

Report No. A-23-02   July 26, 2023

Background

The President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) on December 18, 2014. FISMA provides 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 Offices of Inspector General (OIG) to perform an annual independent evaluation. The Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the Council of Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council, developed the fiscal year (FY) 2023 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. The FY 2023 IG FISMA metrics focused on 20 core IG metrics, 20 supplemental metrics, and cover a period from July 1, 2022, to June 30, 2023.

Objectives

The objectives of this audit were to independently assess the Farm Credit Administration's (FCA) information security program and practices using the metrics identified by DHS and determine the effectiveness of FCA's information security program and practices.

The FCA OIG retained independent public accounting firm Williams Adley & Company-DC, LLP (Williams Adley) to perform the independent audit of FCA's implementation of FISMA for FY 2023 under the Generally Accepted Government Auditing Standards. This report presents the results of that audit. Williams Adley also prepared responses to the annual FISMA reporting metrics for OIGs, which the FCA OIG submitted via DHS's automated application, CyberScope, in accordance with OMB guidance.

The audit found that FCA has an information security program that continues to mature. FCA's information security program is ranked effective based on the auditors' analysis of 20 core metrics and 20 supplemental metrics under the DHS scoring methodology. 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 in CyberScope
Identify	Risk Management	Managed and Measurable
Identify	Supply Chain Risk Management	Defined
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	Consistently Implemented
Respond	Incident Response	Managed and Measurable
Recover	Contingency Planning	Managed and Measurable

Two recommendations remain open from previous FISMA audits. No additional recommendations were made for this year.

TABLE OF CONTENTS

ACRONYMS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
EL	Event Logging
EO	Executive Order
FCA or Agency	Farm Credit Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IG	Inspector General
ISCM	Information Security Continuous Monitoring
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
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SP	Special Publication
Rev	Revision
Williams Adley	Williams, Adley & Company-DC, LLP

OBJECTIVES

The Farm Credit Administration (FCA or Agency) Office of Inspector General (OIG) retained the independent public accounting firm, Williams, Adley & Company-DC, LLP (Williams Adley), to perform an independent audit of FCA's implementation of the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year (FY) 2023. This report presents the results of that audit. Williams Adley also prepared responses to the annual FISMA reporting metrics for OIGs, which the FCA OIG submitted via the Department of Homeland Security's (DHS) automated application in accordance with Office of Management and Budget (OMB) guidance.

The objectives of this audit were to independently assess the FCA's information security program and practices using the metrics identified by DHS and determine the effectiveness of FCA's information security program and practices.

BACKGROUND AND CRITERIA

On December 18, 2014, the President signed FISMA, which reformed the Federal Information Security Management Act of 2002. 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 OIG or by an independent external firm under OIG monitoring. OMB M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements, requires the OIG to report its responses to OMB's annual FISMA reporting questions for OIGs via CyberScope.

OMB, in coordination with the DHS, provides guidance on reporting categories and responds to questions for meeting the current FY's reporting requirements.[1] OMB uses the data to carry out its oversight responsibilities and to prepare its annual report to Congress on the entities' compliance with FISMA. The FY 2023 FISMA Inspector General (IG) metrics focus on 20 "core" metrics and 20 "supplemental" metrics. The core IG metrics were chosen based on their alignment with Executive Order (EO) 14028,[2] "Improving the Nation's Cybersecurity, "as well as recent OMB guidance. This report presents the results of this independent audit.

FISMA requires each agency IG, or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and

---

[1] OMB M-23-02, "Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements," December 2, 2022.
[2] EO 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

WILLIAMS ADLEY

practices of its respective agency. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders worked collaboratively to develop the FY 2023-2024 IG FISMA Reporting Metrics. The FY 2023-2024 IG FISMA Reporting Metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle.

On December 2, 2022, OMB M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements, provided instructions for meeting the FY 2023 FISMA reporting requirements.

According to the memorandum, the FY 2023 reporting presents the first opportunity for an agency IG or independent assessor to evaluate the following group of 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 (NIST Framework)

In response to the growing concern related to cybersecurity, EO 13636[3] was issued in 2013, which requires the development of a set of industry standards and best practices to help organizations manage information security risks to combat cybersecurity challenges. Resulting from this EO was the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).[4] The Cybersecurity Framework[5] provides guidelines for organizations to protect critical infrastructure[6] by using business drivers to direct information security activities and to consider information security risks as part of the organization's risk management processes.

To emphasize the importance of protecting critical infrastructure, EO 13800[7] was issued to hold agency heads accountable for managing cybersecurity risk in their organizations. Specifically, EO 13800 defines effective risk management as requiring agency heads to lead integrated teams of senior executives with expertise in information technology (IT), security, budgeting, acquisition, law, privacy, and human resources. Furthermore, EO 13800 requires agency heads to use the Cybersecurity Framework to manage the agency's cybersecurity risk and hold agency heads

---

[3] EO 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.
[4] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014.
[5] Version 1.1 of the Cybersecurity Framework was published in April 2018 to provide refinements, clarifications, and enhancements to Version 1.0 published in February 2014.
[6] According to EO 13636, critical infrastructure is defined as "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."
[7] EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

accountable for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

The Cybersecurity Framework provides federal agencies with a common structure for identifying and managing information security risks across the enterprise and provides guidance for assessing the maturity of controls to address those risks. The Cybersecurity Framework contains five information security functions that give federal agencies the ability to select and prioritize improvements in information security risk management. The five information security functions are as follows:

- **Identify** – The "identify" function requires the development of organizational understanding to manage information security risk to systems, assets, data, and capabilities.
- **Protect** – The "protect" function requires the development and implementation of appropriate safeguards to ensure delivery of critical services.
- **Detect** – The "detect" function requires the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – The "respond" function requires the development and implementation of appropriate activities to act regarding a detected cybersecurity event.
- **Recover** – The "recover" function requires the development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cybersecurity event.

The five functions (identify, protect, detect, respond, and recover) of the Cybersecurity Framework provide agencies with the structure and guidance to improve their information security program by using an effective risk management strategy to govern and protect their environment. Furthermore, the five functions support recurring risk assessments and validation of business drivers to help agencies implement the necessary information security activities that reflect desired outcomes. Each function places reliance on the development of those preceding it. For example, an organization cannot protect its IT environment properly without first identifying its key information systems and the risks faced by each. Moreover, an organization cannot respond to cybersecurity events if it has not first implemented proper measures to detect them.

FY 2023-2024 IG FISMA Reporting Metrics

The FY 2023 IG FISMA Reporting Metrics emphasize the importance of cybersecurity across federal agencies. OMB, DHS and CIGIE developed the metrics using the NIST Cybersecurity Framework's five information security functions. The metrics give federal agencies the ability to select and prioritize improvements in information security risk management. OMB, DHS, and CIGIE modified the FISMA reporting areas around the five Cybersecurity Framework functions:

1. Identify Function (Risk Management and Supply Chain Risk Management),
2. Protect Function (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training),
3. Detect Function (Information Security Continuous Monitoring),
4. Respond Function (Incident Response), and

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

5. Recover Function (Contingency Planning).

A maturity model summarizes the status of agencies' information security programs and their maturity on a five-level scale (Level 1 to Level 5). Based on the IG FISMA metrics,[8] IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures. The maturity model score of Level 4 (Managed and Measurable) is considered to be an effective level of security at the metric, domain, function, and overall program level.

Identify
o *Risk Management* – The purpose of the risk management domain is to evaluate the maturity of an agency's risk management program. An agency with an effective risk management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.
o *Supply Chain Risk Management (SCRM)* – The purpose of the supply chain risk management domain is to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and SCRM requirements. An agency with an effective SCRM program manages supply chain risks and ensures that third parties adhere to organizational cybersecurity and supply chain requirements; ensures that counterfeit components are detected and prevented from entering the organization's systems; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its program.

Protect
o *Configuration Management* – The purpose of the configuration management domain is to evaluate the maturity of an agency's configuration management program. An agency with an effective configuration management program uses automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.
o *Identity and Access Management* – The purpose of the identity and access management domain is to evaluate the maturity of an agency's identity and access management program. An agency with an effective identity and access management program ensures that all privileged and non-privileged users use strong authentication to access organizational systems; uses automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative

---

[8] CIGIE, DHS, OMB, "FY 2023 Core IG Metrics Implementation Analysis and Guidelines."

5

performance measures on the effectiveness of its identity, credential, and access management program.

o *Data Protection and Privacy* – The purpose of the data protection and privacy domain is to evaluate the maturity of an agency's data protection and privacy program. An effective data protection and privacy program enables an agency to ensure protection of its personally identifiable information (PII) and other agency-sensitive data throughout the data lifecycle; respond to privacy events; develop and maintain enhanced network defenses; and monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its data protection and privacy program.

o *Security Training* – The purpose of the security training domain is to evaluate the maturity of an agency's security training program. An agency with an effective security training program addresses all of its identified knowledge, skills, and abilities gaps; measures the effectiveness of its security training program; and ensures staff consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training activities.

Detect

o *Information Security Continuous Monitoring (ISCM)* – The purpose of the ISCM domain is to evaluate the maturity of an agency's ISCM program. An agency with an effective ISCM program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies, procedures, plans, and strategies.

Respond

o *Incident Response* – The purpose of the incident response domain is to evaluate the maturity of an agency's incident response program. An agency with an effective incident response program uses profiling techniques to measure the characteristics of expected activities on its network and systems so that it can more effectively detect security events; manages and measures the impact of successful events; uses incident response metrics to manage and measure the timely reporting of incident information to organizational officials and external stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.

Recover

o *Contingency Planning* – The purpose of the contingency planning domain is to evaluate the maturity of an agency's contingency planning program. An agency with an effective contingency planning program uses automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities.

WILLIAMS ADLEY

Key Changes to the FY 2023 IG FISMA Reporting Metrics

Reflecting OMB's shift in emphasis away from compliance in favor of risk management-based security outcomes, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls. In response to the threat environment and technology ecosystem, which continue to evolve and change at a faster pace each year, OMB implemented a new framework regarding the timing and focus of assessments in FY 2022. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community.

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. The FY 2023 IG FISMA metrics focused on 20 core and 20 supplemental IG metrics. The FY 2023 core IG metrics were chosen based on alignment with EO 14028, Improving the Nation's Cybersecurity, as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity, including:

- OMB M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements: Agencies are required to report at least 80% of government-furnished equipment through the DHS' Continuous Diagnostics Management program by October 2023. As such, IG metric #2 regarding hardware asset management has been updated to reflect this new requirement.
- DHS Binding Operational Directive (BOD) 23-01, Improving Asset Visibility and Vulnerability: Agencies are required to take specific actions for asset discovery, vulnerability enumeration, and automated reporting to enhance detection by April 2023. As such, IG metrics #2, #20, and #21 regarding hardware asset management, configuration settings, and flaw remediation, respectively, have been updated.
- OMB M-21-30, Protecting Critical Software through Enhanced Security Measures: This memorandum provides guidance on the implementation of security measures for EO critical software. As such, IG metric #3 regarding software asset management has been updated.
- OMB M-22-18, Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices: This memorandum requires agencies to comply with NIST guidance and any subsequent updates related to software supply chain security. As such, IG metric #14 regarding third-party security has been updated to reflect requirements regarding software producer self-attestations.
- OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents: This memorandum directs Agencies to take action to strengthen audit logging, log retention, and log management capabilities. As such, IG metrics #32 and #54 regarding privileged account management and incident detection and analysis, respectively, have been updated to reflect these requirements.
- OMB M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response: This memorandum directs agencies to take action to strengthen their endpoint detection and

response solutions and capabilities. As such, IG metric #37 regarding data exfiltration and enhanced network defenses has been updated to reflect this requirement.

Scoring Methodology

In previous years, IGs have been directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. The same logic was applied at the function and overall information security program level. However, in FY 2021, OMB and CIGIE conducted a pilot to score agencies based on a weighted average for certain priority metrics. One purpose of this pilot was to help evaluate the impacts of these priority metrics and prepare agencies for the possibility of changing the maturity calculation process in the future.

Through analyses of the data obtained through this pilot and the FY 2020 – FY 2022 government-wide IG FISMA reporting, OMB and CIGIE determined that a non-weighted (e.g., calculated) average more closely aligned with the OIG's assessed maturity levels expressed in a numeric format. This result highlights that maturity levels assigned by IGs at the domain, function, and information security program levels align more closely to an approach based on a calculated average than one based on the mode. Further, with the introduction of core metrics in FY 2022, a mode-based scoring approach, where all metrics are weighted equally, may not provide an accurate assessment of maturity in cases where specific domains and function areas may not have a large number of metrics. Therefore, ratings in FY 2023 focus on a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

NIST Risk Management Framework

NIST has established the information security risk management best practices via the Risk Management Framework as detailed in the Special Publication (SP) 800-37, Revision (Rev) 2, Risk Management Framework for Information Systems and Organizations,[9] and NIST SP 800-39, Managing Information Security Risk.[10] The NIST Risk Management Framework provides guidance for federal agencies to establish robust enterprise-wide information security risk management programs to guide the implementation of an information security program. This NIST guidance postulates that establishing effective governance and a formalized approach to information security risk management is the critical first step to achieving an effective information security program.

---

[9] NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018.
[10] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.

Maturity Models

According to the IG FISMA 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 maturity model spectrum is divided into five levels outlined below:

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

According to the FY 2023 IG FISMA metrics, a Level 4, Managed and Measurable, 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 and where quantitative and qualitative performance measures on the effectiveness of said policies, procedures, and strategies are collected across the organization and assessed to make necessary changes.

RESULTS/FINDINGS

Overall Rating

Based on the IG FISMA metric requirements, Williams Adley has concluded that FCA has implemented an effective information security program for FY 2023. FCA continued to improve its information security program and made progress in implementing the majority of the recommendations resulting from previous FISMA audit results.

Additional elements of the information security program include:
- Information security policies and procedures,
- Corrective action processes for significant information security weaknesses,
- Use of a Change Control Board,
- Standard baseline configurations,
- A patch management process,
- Vulnerability and security control assessments,

- Alerts for suspicious activity and devices,
- Weekly security meetings, and
- Continuity of operations plan.

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

Function	Domain	Ranking Assigned in CyberScope
Identify	Risk Management	Level 4: Managed and Measurable
Identify	Supply Chain Risk Management	Level 2: Defined
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 3: Consistently Implemented
Respond	Incident Response	Level 4: Managed and Measurable
Recover	Contingency Planning	Level 4: Managed and Measurable

Identify

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 is composed of the risk management process, which includes ongoing information system authorization, and promotes the concept of near-real-time risk management at the entity level, business process level, and information system level.

The Identify function includes the Risk Management and Supply Chain Risk Management (SCRM) domains. Williams Adley evaluated the domains in the Identify function using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for Level 3, **Consistently Implemented.**

Risk Management

Risk management is the process of identifying, assessing, mitigating, and monitoring risks. An inconsistent and non-comprehensive risk management program creates an operating environment where information security risks could be overlooked and where mitigation strategies may not be implemented. Without fully understanding the complete environment, management may be unknowingly accepting an unacceptable level of risk.

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

The overall maturity level for FCA's risk management program is **Managed and Measurable**. Williams Adley determined FCA's risk management program is effective based on the risk management metrics developed by DHS and related testing performed during this audit.

The current Risk Management program includes the following attributes:
- A current system inventory and categorization of all major systems including systems residing in the cloud,
- Email alerts for unauthorized hardware,
- A list of software approved by the Change Control Board,
- A risk management tool for tracking cybersecurity risks,
- Security controls based on risk that identify minimum baseline controls selected and implemented for internal information systems,
- Independent assessments of controls,
- A process for tracking identified information security weaknesses through plans of action and milestones and tracking their status,
- Regular and timely communications related to information system security risks among IT staff,
- Communication of risks in a timely and consistent manner with senior management, and
- A process for authorizing information systems based on acceptable risks.

WILLIAMS ADLEY

Supply Chain Risk Management

SCRM is the process of identifying, assessing, selecting, and implementing risk management and mitigating control throughout their organizations to help manage supply chain risks.

Williams Adley determined FCA's SCRM program is not effective based on the SCRM metrics developed by DHS. The overall maturity level for FCA's SCRM program is **Level 2 Defined**.

The current SCRM program includes the following attributes:
- A contract desk manual that outlines the procurement policy,
- A listing of standard procurement clauses,
- Change management operating procedures,
- SCRM policies and procedures, and
- A Change Control Board that reviews each proposed change for adverse security risks.

FCA has defined and communicated SCRM policies and procedures; however, FCA has not fully implemented the SCRM policies and procedures. ███

Therefore, no recommendations have been issued.

Protect

The Protect function seeks to develop and implement safeguards to ensure the delivery of critical infrastructure services by supporting the ability to limit or contain the impact of a potential information security event. The Protect function comprises four domains: configuration management, identity and access management, data protection and privacy, and security training.

Williams Adley 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**

Configuration Management

According to NIST SP 800-53, Rev 5, *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 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 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."

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

12

Williams Adley determined FCA's configuration management program is effective based on the configuration management metrics developed by DHS and related testing performed during this audit. The overall maturity rating level for FCA's configuration management program is **Managed and Measurable.**

The configuration management program includes the following attributes:
- An Information Resource Management planning process that guides enterprise-wide IT asset management and investment control,
- A Change Control Board that reviews each proposed change for adverse security risks and configuration impacts,
- Automated alerts that warn of unauthorized hardware on the 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 dissemination or modification of data because they ensure that only approved and authorized personnel have access to FCA information. A lack of an effective identity and access management practice increases the risk of unauthorized system access, whether by internal employees or external attackers, endangering the confidentiality, integrity, and availability of FCA systems.

The overall maturity level for FCA's identity and access management program is **Managed and Measurable**. Williams Adley determined FCA's identity and access management program is effective based on the metrics developed by DHS and related testing performed during this audit.

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,
- Periodic reviews of active accounts,
- Alerts for suspicious account activity,
- Alerts for unauthorized devices connected to the network,
- Multi-factor authentication for all privileged and non-privileged users, and
- Continuous monitoring of privileged accounts.

Data Protection and Privacy

Sensitive information, including PII and sensitive personally identifiable information, should be protected from inappropriate dissemination. Data Protection and Privacy is about preventing the unwanted release of sensitive information and responding to any instances where information is found to be inadvertently shared.

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[11] 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, Appendix I § 4(e)(1), 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[12] by programs and information systems."

The overall maturity level for FCA's data protection and privacy program is **Managed and Measurable**. Williams Adley determined FCA's data protection and privacy program is effective based on the metrics developed by DHS and related testing performed during this audit.

The data protection and privacy program includes the following attributes:
- A comprehensive plan and framework that includes developing additional supporting policies and procedures and addresses OMB A-130 and A-108,
- A breach response plan that includes policies and procedures for data breach reporting, assessment, notification of affected parties due to a data breach, and identifies data breach response team members and incident management team members,
- Annual information security and privacy awareness training to employees and contractors that provides examples of PII and sensitive information and guidance for protecting sensitive information,
- Data at rest, data in transit, media sanitization, and limitation of removable media policies and procedures,
- Restriction on writing to unauthorized devices, and

---

[11] Senior Agency Official for Privacy (SAOP).
[12] Personally, Identifiable Information (PII).

- Implementation of Data Loss Prevention policy and tools.

Security Training

People are often the weakest link in security. Security training helps to ensure that personnel at all levels understand their information security responsibilities 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 organizational security policy and role-based security responsibilities to increase its rate of success in protecting information.

Williams Adley determined FCA's security training program is effective based on the metrics developed by DHS and related testing performed during this audit. The overall maturity level for FCA's security training program is **Managed and Measurable**.

The security training program includes the following attributes:
- Annual IT security awareness training that contained content relative to the Agency,
- Specialized annual IT security awareness training for IT specialists, including individuals with significant security responsibilities,
- IT security training materials for new employee and contractor orientation,
- Status tracking of IT security awareness training to ensure all information system users completed the training,
- Feedback on annual IT security awareness training and documenting frequently asked questions to further inform users, and
- IT security awareness training program through phishing exercises.

Detect

The Detect function of the Cybersecurity Framework enables timely discovery of an information security event. The Detect function comprises one domain — Information Security Continuous Monitoring (ISCM), which seeks to provide visibility into IT assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls.

Williams Adley evaluated the Detect domain, using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for Level 3, **Consistently Implemented**.

Information Security Continuous Monitoring

ISCM enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[13] Without a fully implemented ISCM program, FCA may be unable to detect attempts to damage its systems, resulting in unauthorized access, data loss, operational failure, or unauthorized data modification. FCA would also be unable to develop the key security metrics needed to measure and monitor the effectiveness of its current information security posture.[14]

Williams Adley determined FCA's ISCM domain is not effective based on the ISCM management metrics developed by DHS and related testing performed during this audit. The overall maturity level for FCA's ISCM domain is **Consistently Implemented.**

FCA's ISCM program includes the following attributes:
- An ISCM strategy that provides visibility into IT assets,
- An awareness of vulnerabilities and threats,
- Security alerts,
- 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.

In the FY 2020 FCA FISMA Audit, Williams Adley made a recommendation to improve FCA's ISCM Program. FCA's Office of Information Technology (OIT) considers this recommendation a long-term project that requires significant planning and testing. FCA's OIT continues to make progress in continuous monitoring. FCA's OIT has completed ███████████████████████

Sidebar (maturity levels):

Level 1
Ad-hoc

Level 2
Defined

Level 3
Consistently
Implemented

Level 4
Managed and
Measurable

Level 5
Optimized

---

[13] NIST SP 800-137, ISCM for Federal Information Systems and Organizations, September 2011.

[14] Security posture includes the design and implementation of security plans and the approach the entity takes to information security. It comprises technical and non-technical policies, procedures, and controls to protect the entity from internal and external threats.

WILLIAMS ADLEY

███ As a result, Williams Adley did not make any additional recommendations in this area. The following recommendation will remain open in FY 2023: Williams Adley recommends that the Office of Information Technology ██ ██████████████████

Furthermore, FCA's OIT is making progress to ████████████████████████████ ████████████████████████████████ in order to resolve one of our FY 2022 FISMA audit recommendations. ██ ███ ███████████████████████████████████████

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. Williams Adley evaluated the domains in the Respond function using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for Level 4, **Managed and Measurable.**

Incident Response

NIST SP 800-61, Rev 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; and post-incident activity.

The overall maturity level for FCA's incident response program is **Managed and Measurable**. Williams Adley determined FCA's incident response program is effective based on the metrics developed by DHS and related testing performed during this audit. ███████████████████████████████████████ ███ ███ ███ ██████████ Therefore, no recommendation has been issued.

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

WILLIAMS ADLEY

The 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 IT equipment or sensitive information that is suspected to be missing, lost, or stolen, or suspected security incidents,
- Risk assessment for all incidents,
- A threat alert log for tracking potential incidents,
- Collaboration and 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

The Recover function seeks to reduce the negative impact of an information security event through the timely recovery of normal operations via contingency planning.

The Recover function includes the Contingency Planning domain. Williams Adley evaluated the domain 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.

In FY 2023, FCA tested the set of documented Information System Contingency Plans for the ▮▮▮

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

Contingency Planning

According to NIST SP 800-34, Rev 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.

Williams Adley determined FCA's contingency planning program is effective based on the metrics developed by DHS and related testing performed during this audit. The overall maturity level for FCA's contingency planning is **Managed and Measurable**.

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,
- Participation by senior executives and IT personnel during periodic continuity exercises,

18

- System-specific information system contingency plans and business impact analyses,
- An information system backup strategy that includes alternate storage facilities,
- Self-evaluation of Agency performance following an annual continuity exercise,
- Identification of mission essential functions, and
- An alternate recovery site to facilitate continuity of mission essential functions.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objectives of this audit were to independently assess the Farm Credit Administration's (FCA) information security program and practices using the metrics identified by DHS and determine the effectiveness of FCA's information security program and practices.

In support of this objective, Williams Adley conducted an independent audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the FCA's implementation of FISMA[15] for FY 2023.. In reporting the CyberScope results we relied on OMB M-23-03, FY 2023 Guidance on Federal Information Security and Privacy Management Requirements.

Scope

The audit focused on reviewing FCA's implementation of FISMA for FY 2023. The audit 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 of a representative subset of FCA's information systems, including contractor systems and systems provided by other federal agencies. Based on a risk-based methodology, Williams Adley selected the following three systems:

-
-
-

Methodology

Williams Adley performed qualitative analyses to assess the effectiveness of the FCA's efforts to secure its information systems. The audit included an assessment of the NIST Cybersecurity Framework Function Levels, as specified in the FY 2023 IG FISMA Reporting Metrics:

- Identify (Risk Management)
- Identify (Supply Chain Risk Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- Protect (Date Protection and Privacy)

---

[15] Public Law. No. 113-283, FISMA, December 18, 2014..

WILLIAMS ADLEY

- Protect (Security Training)
- Detect (Information Security Continuous Monitoring)
- Respond (Incident Response)
- Recover (Contingency Planning)

FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. To ensure the adequacy and effectiveness of these controls, FISMA requires an independent annual review of the information security program and the head of the agency to report those results to OMB. The FY 2023 IG FISMA Reporting Metrics developed by the OMB, DHS, and CIGIE is intended to provide guidance on the OIG's annual evaluations, as required by the FISMA, 44 U.S. Code, section 3555(j).

Williams Adley performed this audit from March through June 2023. William Adley conducted this audit in accordance with GAGAS. GAGAS requires that Williams Adley obtain sufficient evidence to provide a reasonable basis for its findings and conclusions based on the auditor's evaluation objectives.

To perform this audit, Williams Adley interviewed FCA senior management and employees, remotely observed FCA's operations, obtained evidence to support Williams Adley's conclusions and recommendations, tested the effectiveness of controls, conducted sampling where applicable, and collected written documents to supplement observations and interviews. Williams Adley provided a draft report to FCA management on July 19, 2023. An exit conference was conducted on July 21, 2023.

Use of Computer Processed Data

During the audit, Williams Adley used computer-processed data to obtain samples and information regarding the existence of information security controls. For example, Williams Adley obtained system-generated reports of the information system inventory from FCA personnel. These reports were used to support the audit procedures in the risk management IG FISMA metric domain. Williams Adley assessed the reliability of the computer-generated data primarily by comparing selected data with source documentation, data from prior years, inquiring with FCA personnel, and observing the selected data being generated. Where applicable, Williams Adley determined that the information was sufficiently reliable for assessing the adequacy of related information security controls.

Sampling Methodology

For all samples selected during the audit, Williams Adley used non-statistical sampling techniques where applicable and appropriate. As guidance, Williams Adley used the American Institute of

Certified Public Accountants Audit Guide Audit Sampling.[16] This guidance assists in applying sampling in accordance with auditing standards.

With respect to the sampling methodology employed, standards indicate that either a statistical or judgmental sample can yield sufficient and appropriate evidence. Based on professional judgement, Williams Adley did not use statistical sampling during this audit. Williams Adley employed another type of sample permitted by standards—namely, a non-statistical sample known as a judgmental sample. A judgmental sample is a sample selected by using discretionary criteria rather than criteria based on the laws of probability. In this audit, Williams Adley has taken great care in determining the criteria to use for sampling based on its judgement of risk. Moreover, Williams Adley used, whenever practicable, random numbers to preclude the introduction of any bias in sample selection although a non-statistical technique was used. Williams Adley acknowledges that it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist in other information systems that were not tested. However, a prudent person without any basis in fact would not automatically assume that these deficiencies are non-existent within other systems. Such a supposition would be especially ill-advised for an issue as important as information security.

Evaluation, testing, and analysis were performed in accordance with guidance from the following:

- Chief Financial Officers Council, Enterprise Risk Management Playbook
- Chief Information Officer Council/Chief Acquisition Officer Council, Cloud Computing Contract Best Practices
- GAGAS
- Internet Security Top 18 Security Controls
- Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity & Incident Response Playbooks
- CISA Cybersecurity Incident and Vulnerability Response Playbooks
- CISA Zero Trust Maturity Model
- DHS BOD 18-02
- DHS BOD 19-02
- DHS BOD 22-01
- DHS BOD 23-01
- Security Executive Directive 19-01
- EO 14028: Improving the Nation's Cybersecurity
- FCA's policies and procedures relating to the nine FISMA domains
- E-Government Act of 2002
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance
- Federal Information Processing Standards 199

---

[16] American Institute of Certified Public Accountants Audit Guide, Audit Sampling, March 1, 2014.

WILLIAMS ADLEY

- Federal Information Processing Standards 201-2
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- Federal Acquisition Supply Chain Security Act of 2018
- FY 2023 Chief Information Officer Federal Information Security Modernization Act Metrics
- National Cybersecurity Workforce Framework
- NIST Cybersecurity Framework
- NIST Interagency or Internal Report 8011
- NIST Interagency or Internal Report 8276
- NIST Interagency or Internal Report 8286
- NIST SP 800-18
- NIST SP 800-34, Rev 1
- NIST SP 800-37, Rev 2
- NIST SP 800-39
- NIST SP 800-40, Rev 3
- NIST SP 800-50
- NIST SP 800-53, Rev 5
- NIST SP 800-61, Rev 2
- NIST SP 800-63-3, 63A, B, and C
- NIST SP 800-70
- NIST SP 800-128
- NIST SP 800-137
- NIST SP 800-152
- NIST SP 800-157
- NIST SP 800-207
- NIST SP 800-218
- OMB Circular No. A-123
- OMB Circular No. A-130
- OMB M-14-03
- OMB M-16-17
- OMB M-22-18
- OMB M-19-03
- OMB M-19-17
- OMB M-20-04
- OMB M-21-07
- OMB M-21-30
- OMB M-21-31
- OMB M-22-05
- OMB M-22-09
- US-Computer Emergency Readiness Team, Incident Response Guidelines

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:

Phone:	**(800) 437-7322 (Toll-Free)**
	(703) 883-4316
Fax:	**(703) 883-4059**
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**.