Farm Credit Administration

Office of Inspector General

Audit Report

The Farm Credit Administration's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2021

A-21-02

October 27, 2021

FCAOIG

Farm Credit Administration
Office of Inspector General

FCAOIG

Farm Credit Administration
Office of Inspector General

October 27, 2021

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

Dear Chairman Smith and Board Member Hall:

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 2021 FISMA review. The contract required Williams Adley to follow the Fiscal Year 2021 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 66 metrics under the Department of Homeland Security's scoring methodology. Williams Adley reported that FCA improved multiple aspects of its information security program, including enhancing the data protection and privacy program. Williams Adley made three recommendations that will assist FCA in improving the effectiveness of its information security program.

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 dated October 27, 2021, 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

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

Enclosure

EXECUTIVE SUMMARY

The Farm Credit Administration's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2021

Report No. A-21-02

October 27, 2021

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) 2021 Inspector General FISMA Reporting metrics. The FY 2021 metrics are aligned with the five function areas in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover.

Objectives

The objectives of this audit were to independently assess the Farm Credit Administration's (FCA) information security program 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 2021 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 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 66 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	Ad-Hoc
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	Defined

Williams Adley made three new recommendations related to, Supply Chain Risk Management, Configuration Management, and Incident Response, and one recommendation from FY 2020 remained open. The recommendations were provided to the Office of Information Technology to strengthen and improve FCA's information security program.

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

TABLE OF CONTENTS

ACRONYMS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
DRP	Disaster Recovery Plan
FCA or Agency	Farm Credit Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IT	Information Technology
ISCM	Information Security Continuous Monitoring
ISCPs	Information System Contingency Plans
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
PPM	Policies and Procedures Manual
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management

SP	Special Publication
Rev	Revision
TIC	Trusted Internet Connection
VDP	Vulnerability Disclosure Policy

OBJECTIVE

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) 2021. 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 the audit were to perform an independent audit of the FCA's implementation of FISMA and to determine the effectiveness of the information security program for FY 2021.

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. OMB Memorandum 21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements, dated November 9, 2020, requires the OIG to report their 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 fiscal year'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.

[1] OMB, Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements, Memorandum M-21-02, November 9, 2020.

Cybersecurity Framework (NIST Framework)

In response to the growing concern related to cybersecurity, Executive Order 13636[2] 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 Executive Order was the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" (Cybersecurity Framework).[3] The Cybersecurity Framework[4] provides guidelines for organizations to protect critical infrastructure[5] 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, Executive Order 13800[6] was issued to hold agency heads accountable for managing cybersecurity risk in their organizations. Specifically, Executive Order 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, Executive Order 13800 requires agency heads to use the Cybersecurity Framework to manage the agency's cybersecurity risk and hold agency heads 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.

[2] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.

[3] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014.

[4] 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.

[5] According to Executive Order 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."

[6] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

- **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 (5) 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 (5) 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 correctly 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 2021 Inspector General (IG) FISMA Reporting Metrics

FISMA requires OMB to ensure that guidance is developed for the independent audit of agency information security programs. On May 13, 2021, the OMB, DHS, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) released the "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1."[7]

This guidance provides metrics to be used to gauge the maturity of agency practices in connection with the nine domains that are organized around the five information security functions outlined in the Cybersecurity Framework:

Identify

- *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.
- *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 organization's systems; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its program.

[7] OMB, DHS, and CIGIE, "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics," May 12, 2021.

Protect

- *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.
- *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 performance measures on the effectiveness of its identity, credential, and access management program.
- *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.
- *Data Protection and Privacy (DPP)* – 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.

Detect

- *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

- *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

- *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.

Key Changes to the FY 2021 IG FISMA Reporting Metrics

The FY 2021 FISMA reporting metrics included changes to 1) focus on increasing the maturity of the Federal government's SCRM practices through the introduction of a new SCRM domain within the Identify function, and 2) improve vulnerability identification, management, and remediation.

The new SCRM domain introduces five questions (#12-16) which focus on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and SCRM requirements. The new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision (Rev) 5, Security and Privacy Controls for Information Systems and Organizations released in September 2020, with updates made in December 2021. To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5, in accordance with OMB A-130, the SCRM domain will not be considered for the purposes of the Identify framework function rating.

On September 2, 2020, OMB released Memorandum M-20-32, Improving Vulnerability Identification, Management, and Remediation**,** which provides guidance to federal agencies on collaborating with members of the public to find and report vulnerabilities on federal information systems. On the same day, DHS published Binding Operational Directive 20-01, Develop and Publish a Vulnerability Disclosure Policy, which provides guidance on the development and publishing of an agency's vulnerability disclosure policy (VDP) and supporting handling procedures. To address these items, the IG FISMA Reporting Metrics introduced a new question (#24) that focuses on determining whether agencies utilize a VDP as part of their vulnerability management program for internet-accessible federal systems.

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, Rev 2, Risk Management Framework for Information Systems and Organizations,[8] and NIST SP 800-39, Managing Information Security Risk.[9] The NIST Risk Management Framework provides guidance for federal agencies to establish a 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.

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 2021 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."

[8] NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018.

[9] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.

RESULTS/FINDINGS

Overall Rating

Based on the IG FISMA metric requirements, Williams Adley has concluded that FCA has implemented an effective information security program in FY 2021. FCA continued to improve its information security program and made progress in implementing the majority of the recommendations resulting from previous FISMA evaluations.

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,
- Continuous monitoring processes,
- 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 CyberScope's scoring. Each function and domain are discussed in more detail in the subsequent sections of this report.

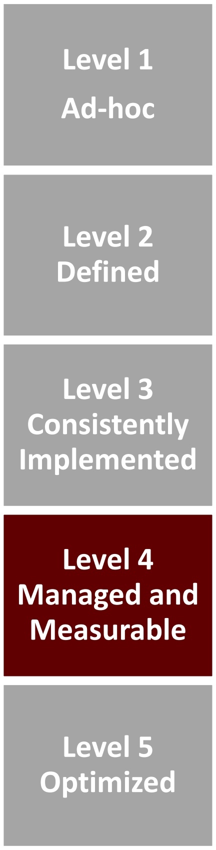
Function	Domain	Ranking Assigned in CyberScope
Identify	Risk Management	Level 4: Managed and Measurable
Identify	Supply Chain Risk Management	Level 1: Ad-Hoc
Protect	Configuration Management	Level 4: Managed and Measurable
Protect	Identity and Access Management	Level 4: Managed and Measurable
Protect	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 2: Defined

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 domains. However, the Supply Chain Risk Management domain was not used to evaluate the maturity of FCA's Information security program in 2021. 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 4, **Managed and Measurable**.



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.

Williams Adley determined FCA's risk management program is **Managed and Measurable** 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.

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 **Ad-Hoc** based on the SCRM metrics developed by DHS and related testing performed during this audit. The SCRM domain was added to the IG FISMA metrics in FY 2021. These metrics were not used to evaluate the maturity of agency's information security program in 2021 to provide the organization with sufficient time to implement NIST SP 800-53, Rev 5. However, Williams Adley determined the conditions below as an area of improvement in preparation for the FCA's implementation of NIST SP 800-53 Rev 5 in FY 2022.

The current SCRM program includes the following attributes:

- A contract desk manual that outline the procurement policy,
- A listing of standard procurement clauses,
- Change management operating procedures, and
- A Change Control Board that reviews each proposed change for adverse security risks.

Condition:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Cause: [redacted]

Criteria:

- NIST SP 800-53 Rev 5, Security and Privacy Controls for Federal Information Systems and Organization: [redacted]
  - [redacted];
  - [redacted]
  - [redacted].
- NIST SP 800-53, Rev 4: [redacted]
- NIST SP 800-53, Rev 5: [redacted]
- NIST SP 800-53, Rev 5: [redacted]
- NIST SP 800-53, Rev 5: [redacted]
- NIST SP 800-53, Rev 5: [redacted]
- NIST SP 800-53, Rev 5: [redacted]
- [redacted]
- [redacted]

Effect: [redacted]

Recommendation 1: William Adley recommends that the Office of Information Technology [redacted]

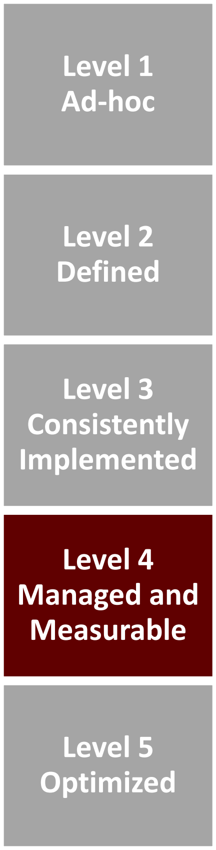
OIT Response: FCA OIT Management agrees with the recommendation and will [redacted] OIT's estimated completion date for these actions is [redacted].

Williams Adley Response: The corrective actions will be evaluated during the OIG recommendation closeout process.

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.

In FY 2021, the Protect function operated at Level 4: Managed and Measurable, which reflects the Protect function's four domains. Configuration Management domain operated at Level 3: **Consistently Implemented**. The other three domains — identity and access management, data protection and privacy, and security training, operated at Level 4: **Managed and Measurable.**



Configuration Management

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

Williams Adley determined FCA's configuration management program is not 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.

Condition:

- [redacted]

[redacted]

- [redacted]

Cause: [redacted]

Criteria

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Effect: [redacted]

Recommendation 2: Williams Adley recommends that the Office of Information Technology [redacted]

OIT Response: FCA OIT Management agrees with the recommendation and will [redacted] OIT's estimated completion date for these actions is [redacted].

Williams Adley Response: The corrective actions will be evaluated during the OIG recommendation closeout process.

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 include 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 most 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 (DPP) 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[10] 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[11] 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 include the following attributes:

[10] Senior Agency Official for Privacy (SAOP)

[11] Personally, Identifiable Information (PII)

- 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, and
- Restriction on writing to unauthorized devices.

Security Training

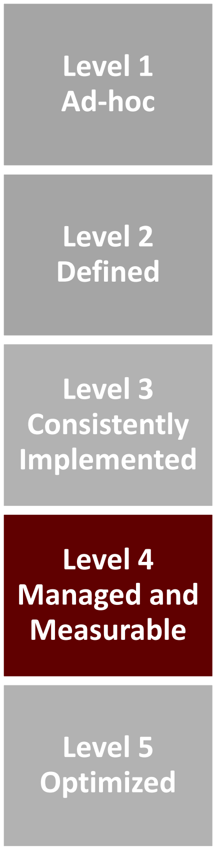
People are often the weakest link in security. Security training helps to ensure that personnel at all levels understand their information security responsibilities to properly use and protect the information and the resources entrusted to them. Therefore, a well-defined security training process must 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
- Effective 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 4, **Managed and Measurable**.

Information Security Continuous Monitoring (ISCM)

ISCM enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[12] 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.[13]

Williams Adley determined FCA's ISCM domain is 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 **Managed and Measurable.**

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 [redacted]

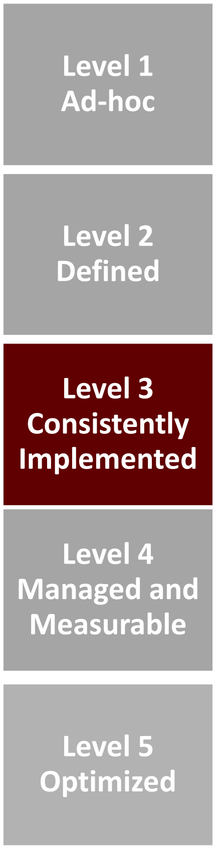
[12] NIST SP 800-137, ISCM for Federal Information Systems and Organizations, September 2011.

[13] 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.

[redacted] Therefore, Williams Adley did not make any additional recommendations in this area. The following recommendation remains open in FY 2021: Williams Adley recommends that the Office of Information Technology [redacted]

Respond

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


Level 1 Ad-hoc

Level 2 Defined

Level 3 Consistently Implemented

Level 4 Managed and Measurable

Level 5 Optimized

The Respond function includes the Incident Response domain. Williams Adley evaluated the domain using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for Level 3, **Consistently Implemented.**

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 **Consistently Implemented.** Williams Adley determined FCA's incident response program is not effective based on the metrics developed by DHS and related testing performed during this audit.

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.

Conditions:

- [redacted].
- [redacted]

- ○ [redacted]
- ○ [redacted]
- ○ [redacted]
- ○ [redacted]
- ○ [redacted]

Cause:

- [redacted]

Criteria:

- NIST SP 800-61, Rev 2, Computer Security Incident Handling Guide
- [redacted]
- [redacted]

Effect: [redacted]

Recommendation 3: William Adley recommends that the Office of Information Technology [redacted]

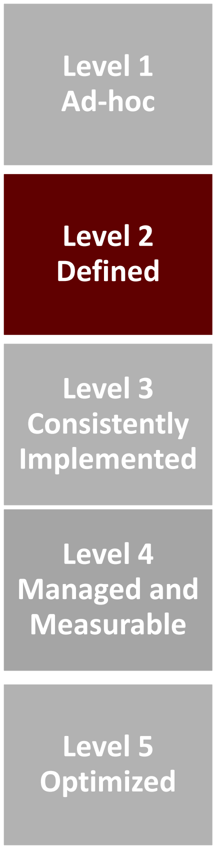
OIT Response: FCA OIT Management agrees with the recommendation and will [redacted] OIT's estimated completion date for these actions is [redacted]

Williams Adley Response: The corrective actions will be evaluated during the OIG recommendation closeout process.

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 2, **Defined,** which is defined as not effective.



[redacted]

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 not effective based on the metrics developed by DHS and related testing performed during this audit. The overall maturity level for FCA's contingency program is **Defined**.

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,
- 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.

[redacted]

OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

The objective was to perform an independent audit of the FCA's implementation of FISMA[14] for FY 2021. In support of this objective, Williams Adley conducted the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). In reporting the CyberScope results we relied on OMB 21-02, FY 2020 – 2021 Guidance on Federal Information Security and Privacy Management Requirements, reporting guidelines.

Scope

The audit focused on reviewing FCA's implementation of FISMA for FY 2021. 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 identified three inhouse maintained systems. [redacted]:

- [redacted]
- [redacted]
- [redacted]

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 2021 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)
- 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

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

annual review of the information security program and the head of the agency to report those results to OMB. The FY 2021 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 May through September 2021 and 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 to evaluate managerial effectiveness and operational controls in accordance with NIST and OMB guidance. Williams Adley remotely observed FCA's operations, obtained evidence to support Williams Adley's conclusions and recommendations, tested the effectiveness of established or defined controls, conducted sampling where applicable, and collected written documents to supplement observations and interviews. Williams Adley provided a draft report to FCA management on October 19, 2021. An exit conference was conducted on October 26, 2021.

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.[15] 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

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

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
- Cybersecurity Sprint
- FCAs policies and procedures relating to the nine FISMA domains
- Cybersecurity Strategy and Implementation Plan
- Department of Homeland Security Binding Operational Directive 19-02
- Department of Homeland Security Binding Operational Directive 17-01
- Department of Homeland Security Cyber Incident Reporting Unified Message
- E-Government Act of 2002
- Federal Acquisition Regulation sections 39.101, 105, 52.224-1, 52.224-2, and 52.239-1
- Federal Continuity Directive 1
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Enterprise Architecture Framework
- Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance
- Federal Information Processing Standards 199
- Federal Information Processing Standards 201-2
- Federal Information Security Modernization Act of 2014
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
- Homeland Security Presidential Directive 12
- Government Accountability Office, Standards for Internal Control in the Federal Government
- National Archives and Records Administration, Guidance on Information Systems Security Records
- National Cybersecurity Workforce Framework
- National Insider Threat Policy
- National Institute of Standards and Technology Cybersecurity Framework
- National Institute of Standards and Technology (NIST) SP 800-30
- National Institute of Standards and Technology (NIST) SP 800-34
- National Institute of Standards and Technology (NIST) SP 800-37, Rev 2
- National Institute of Standards and Technology (NIST) SP 800-39

- National Institute of Standards and Technology (NIST) SP 800-40, Rev 3
- National Institute of Standards and Technology (NIST) SP 800-44
- National Institute of Standards and Technology (NIST) SP 800-50
- National Institute of Standards and Technology (NIST) SP 800-53, Rev 4
- National Institute of Standards and Technology (NIST) SP 800-60
- National Institute of Standards and Technology (NIST) SP 800-61, Rev 2
- National Institute of Standards and Technology (NIST) SP 800-63
- National Institute of Standards and Technology (NIST) SP 800-83
- National Institute of Standards and Technology (NIST) SP 800-84
- National Institute of Standards and Technology (NIST) SP 800-86
- National Institute of Standards and Technology (NIST) SP 800-122
- National Institute of Standards and Technology (NIST) SP 800-128
- National Institute of Standards and Technology (NIST) SP 800-137
- National Institute of Standards and Technology (NIST) SP 800-161
- National Institute of Standards and Technology (NIST) SP 800-181
- National Institute of Standards and Technology (NIST) SP 800-184
- Office of Management and Budget Circular No. A-11
- Office of Management and Budget Circular No. A-123
- Office of Management and Budget Circular No. A-130, Appendix I
- Office of Management and Budget, Memorandum 04-25
- Office of Management and Budget, Memorandum 08-05
- Office of Management and Budget, Memorandum 14-03
- Office of Management and Budget, Memorandum 14-04
- Office of Management and Budget, Memorandum 16-03
- Office of Management and Budget, Memorandum 16-04
- Office of Management and Budget, Memorandum 16-17
- Office of Management and Budget, Memorandum 17-09
- Office of Management and Budget, Memorandum 17-12
- Office of Management and Budget, Memorandum 17-25
- Office of Management and Budget, Memorandum 18-02
- Office of Management and Budget, Memorandum 19-02
- Office of Management and Budget, Memorandum 19-03
- Office of Management and Budget, Memorandum 19-17
- Office of Management and Budget, Memorandum 20-04
- Office of Management and Budget, Memorandum 20-32
- Office of Management and Budget, Memorandum 21-02
- OMB Circular M-19-26, Update to the Trusted Internet Connections (TIC) Initiative;
- Presidential Policy Directive - 41
- Privacy Act of 1974, as amended
- SANS Institute, Critical Security Controls
- Executive Order 13636, Improving Critical Infrastructure Cybersecurity
- Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- US-Computer Emergency Readiness Team, Federal Incident Notification & Response

Guidelines

- US-Computer Emergency Readiness Team, Incident Response Guidelines