Farm Credit Administration

Office of Inspector General

Evaluation Report

2019 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act

E-19-01

October 30, 2019

FCAOIG

Farm Credit Administration
Office of Inspector General

EXECUTIVE SUMMARY

2019 Evaluation of FCA's Compliance with FISMA

Report No. E-19-01 October 30, 2019

Background

The President signed into law the Federal Information Security Modernization Act (FISMA) of 2014 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 OIGs to perform an annual independent evaluation. The Office of Management and Budget, 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) 2019 IG FISMA Reporting metrics. The FY 2019 metrics are aligned with the five function areas in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover.

Objectives

The objective of this evaluation was to independently assess FCA's information security program using the metrics identified by DHS and determine the effectiveness of FCA's information security program and practices.

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

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

Function	Domain	Ranking Assigned in CyberScope
Identify	Risk Management	Managed and Measurable
Protect	Configuration Management	Managed and Measurable
Protect	Identity and Access Management	Consistently Implemented
Protect	Data Protection and Privacy	Ad Hoc
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

We made two recommendations to the Office of Information Technology (OIT) to strengthen and improve the Agency's information security and privacy program related to updating the Agency's information security policy and Information Security Continuous Monitoring Strategy.

TABLE OF CONTENTS

ACRONYMS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DHS	Department of Homeland Security
FCA or Agency	Farm Credit Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IT	Information Technology
ISCM	Information Security Continuous Monitoring
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
SP	Special Publication

BACKGROUND

The President signed the Federal Information Security Modernization Act (FISMA) of 2014 into law on December 18, 2014.[1] 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 the Office of Inspector General (OIG) to perform an annual independent evaluation. This includes testing a

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

representative subset of the Agency's information systems and assessing the effectiveness of information security policies, procedures, and practices of the agency.

The Office of Management and Budget (OMB) issued Memorandum M-19-02 on October 25, 2018, with guidance for complying with FISMA's annual reporting requirements. Results of the Chief Information Officer (CIO) and OIG assessments are reported to the Department of Homeland Security (DHS) through CyberScope.

DHS issued the Inspector General FISMA Reporting Metrics on April 9, 2019. The Inspector General Reporting Metrics were developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer Council. The fiscal year (FY) 2019 OIG FISMA metrics leverage the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as a standard for managing and reducing cybersecurity risks and are organized around the framework's five functions: Identify, Protect, Detect, Respond, and Recover. Each of the Cybersecurity Framework security functions are supported by eight domains. The eight domains contain 67 individual metrics.

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

OIGs evaluate agency progress for each metric. OMB, DHS, and CIGIE worked together over the past few years to transition the metrics to a maturity model approach. During FY 2019, the most significant change to the metrics were additional maturity indicators and criteria references regarding the evaluation of the effectiveness of agencies' High Value Asset programs. High Value Assets are information or information systems that relate to one or more of the following categories: high value to the Government or its adversaries, mission essential, critical function to maintaining the security and resilience of the Federal civilian enterprise. FCA does not have any High Value Assets.

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

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

Top Management Challenge

Information Technology (IT) Security and Management was one of the most frequently reported challenges identified by CIGIE in its April 2018 report, *Top Management and Performance Challenges Facing Multiple Federal Agencies*. The FCA OIG also identified IT and Data Quality and Analysis as two of five top management challenges facing FCA.

The IT challenge is the ability to leverage investments in IT while maintaining a secure environment. FCA must protect its IT systems and data from the risks of unauthorized access, use, disclosure, disruption, modification, or destruction. While cybersecurity threats are increasing, FCA is increasingly reliant on IT systems to identify and analyze potential risks from the sensitive financial data that the Agency receives from the Farm Credit System. Hence, it is imperative that FCA has the necessary IT tools and staff to protect its systems and data from cybersecurity threats and to operate more efficiently and effectively. At the same time, the Agency must be prudent and responsible with its spending. The Data Quality and Analysis challenge is the ability to obtain consistent, quality data vital to the FCA's mission to ensure the Farm Credit System remains a dependable source of credit for agriculture and rural America.

RESULTS/FINDINGS

The OIG performed an independent evaluation of the FCA's information security program and determined FCA's overall information security program was effective. FCA utilizes a risk-based approach to information security and security controls. The information security program contains

identity and access management, security and privacy training, and incident response programs. 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 and tests.

We reported the results of our review 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
Protect	Configuration Management	Level 4: Managed and Measurable
Protect	Identity and Access Management	Level 3: Consistently Implemented
Protect	Data Protection and Privacy	Level 1: Ad Hoc
Protect	Security Training	Level 4: Managed and Measurable
Detect	Information Security Continuous Monitoring	Level 3: Consistently Implemented
Respond	Incident Response	Level 4: Managed and Measurable
Recover	Contingency Planning	Level 4: Managed and Measurable

During our review, we found that FCA implemented a computer security program designed to manage identified computer risks and vulnerabilities. To support this program, FCA issued Policies and Procedures Manual (PPM) Section 902, *Computer Security Program*, on December 1, 2010.

The Implementing Procedures for PPM 902 include roles and responsibilities as well as guidance about threats and risks associated with the use of information systems. The implementing procedures state that it will be reviewed and updated annually or when certain changes occur, such as changes in roles and responsibilities, legislation, governing policies, vulnerabilities, risks, and threats. This policy references the Federal Information Security Management Act of 2002, which was amended by the Federal Information Security Modernization Act of 2014. Since this PPM addresses the overall information security program and affects all the domains, we determined OIT needs to update this nine-year-old policy.

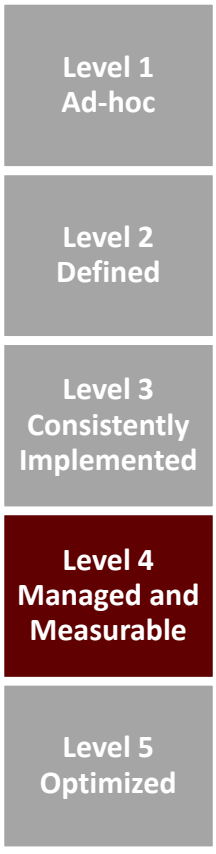
Recommendation 1: We recommend the Office of Information Technology complete its update of Policies and Procedures Manual Section 902, *Computer Security Program*.

Agency Response: OIT agreed with the recommendation. OIT will complete the update of PPM 902 and publish it on FCA's internal policies and procedures site.

OIG Response: The OIG concurs with OIT's planned actions.

Identify

The information security function area for Identify includes the Risk Management domain. We evaluated the domain 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**, which is defined as effective.



Risk Management

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

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

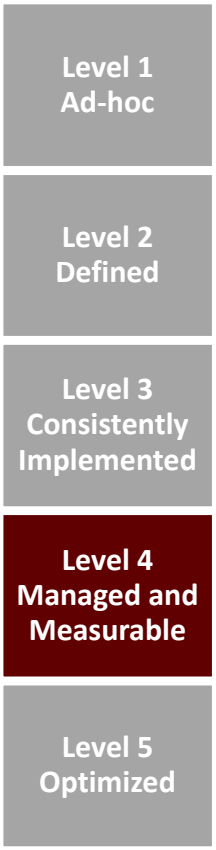
FCA's risk management strategy focuses on operational risks that may inhibit the ability of its IT assets to support FCA mission-essential functions. FCA's strategy is to use a continuous process of identifying, analyzing, and communicating risks to stakeholders. Risks are identified through various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

The 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 to track operational risks,
- Security controls based on risk that identify minimum baseline controls selected and implemented for internal 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.

Protect

The information security function area for Protect includes the following domains: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. We evaluated the domains in the Protect function using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for Level 4, **Managed and Measurable**, which is defined as "Effective."



Configuration Management

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

We determined FCA's configuration management program is effective based on the configuration management metrics developed by DHS and related testing we performed during this evaluation. The overall maturity rating level for FCA's configuration management program is **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,
- A standard baseline configuration for workstations and servers,
- Automated alerts that warn of unauthorized hardware on the network,
- Routine scanning and remediation of system vulnerabilities,
- Automated processes for identification and installation of patches, and
- A process for approving deviations from standard configuration.

Identity and Access Management

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

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

The identity and access management program includes the following attributes:

- Certification that employees and contractors have read the Agency's policy on information security,
- System access based on least privilege,
- Automated mechanisms for account management,
- 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

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

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

> "Develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy[2] 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 SAOP's 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[3] by programs and information systems."

The overall maturity level for FCA's data protection and privacy program is **Ad Hoc**. We determined FCA's data protection and privacy program is not effective based on the metrics developed by DHS and related testing we performed during this evaluation.

The data protection and privacy program include 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, and notification of affected parties due to a data breach, as well as 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,
- Encryption of laptops, and
- Restriction of writing to unauthorized devices.

The CIO was designated the SAOP. In addition, in May 2019, FCA hired its first, dedicated full-time Privacy Officer. The new Privacy Officer conducted a comprehensive review of FCA's privacy program and identified primary risks that will be the initial areas of focus for the privacy program during the next year. Additionally, the Privacy Officer participates in risk management processes such as the Change Control Board.

During the FY 2018 FISMA evaluation, we made several recommendations to improve FCA's data protection and privacy program. The following recommendations remain open from that review:

[2] Senior Agency Official for Privacy (SAOP)
[3] Personally Identifiable Information (PII)

- FCA needs to develop and communicate policies and procedures that identifies the inventory of PII and other sensitive data collected, used, and maintained that needs increased protection.
- FCA needs to formalize policies and procedures for:
    - Encryption of data at rest,
    - Encryption of data in transit,
    - Limitation of transfer to removable media, and
    - Sanitization of digital media prior to disposal or reuse.
- FCA needs to develop policies and procedures related to preventing data exfiltration.

Security Training

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

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

The security training program includes the following attributes:

- Annual IT security awareness training that contained content relative to the Agency,
- Specialized, role-based annual IT security awareness training for IT specialists, including individuals with significant security responsibilities,
- IT security training materials for new employee and contractor orientation,
- Tracking the status of IT security awareness training to ensure all information system users completed the training,
- Obtaining feedback on annual IT security awareness training and documenting frequently asked questions to further inform users,
- Measuring the effectiveness of its IT security awareness training program through phishing exercises, and
- Two Certified Information System Security Professionals in OIT.

Detect

The information security function area for Detect includes the following domain: Information Security Continuous Monitoring (ISCM). We evaluated the domain, Detect, using the guidance provided by DHS. Based on DHS's scoring methodology, FCA met the criteria for Level 3, **Consistently Implemented**.

Information Security Continuous Monitoring

NIST SP 800-137 states, "Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

We determined FCA's ISCM program is not effective based on the ISCM management metrics developed by DHS and related testing we performed during this evaluation. The overall maturity level for FCA's information security continuous monitoring program is Level 3, **Consistently Implemented**. Within the context of the DHS maturity model, Level 4, Managed and Measurable, is considered an effective level of security.

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.

FCA's overarching ISCM program addresses all Agency information systems and is based on risk. However, FCA's ISCM Strategy is four years old and signed by the former CIO. In the past four years, FCA's information security program has gone through significant changes, including the hiring of a new CIO, implementing new security tools, reorganizing the office structure, and increasing the use of contractors. For FCA's ISCM program to mature to Level 4 and be considered effective, FCA needs to update its ISCM Strategy and transition to ongoing security control assessments and authorizations. OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, states, "Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems." This includes the ongoing authorization of common controls inherited by organization information systems. OMB M-14-03 further states, "The complete transition to ongoing authorization should be implemented in accordance with the specific transition criteria established by agencies." OIT has

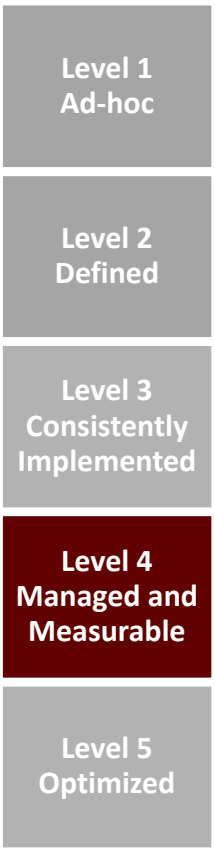
a process for performing security control assessments and granting system authorizations over a three-year cycle. However, OIT has not transitioned to ongoing assessments and authorizations.

Recommendation 2: We recommend the Office of Information Technology update the Information Security Continuous Monitoring Strategy, including the transition to ongoing security control assessments and authorizations and development of performance measures.

Agency Response: OIT agreed with the recommendation. OIT will continue to update the ISCM Strategy to include the transition to ongoing security controls assessments and authorizations and development of performance measures.

OIG Response: The OIG concurs with OIT's planned actions.

Respond



The information security function area for Respond includes the Incident Response domain. We 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**.

Incident Response

NIST SP 800-61, Revision 2 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**. We determined FCA's incident response program is effective based on the metrics developed by DHS and related testing we performed during this evaluation.

The incident response program includes the following attributes:

- A 24-hour 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,
- 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 information security function area for Recover includes the Contingency Planning domain. We 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.

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 Revision 1, "Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods."

We determined FCA's contingency planning program is effective based on the metrics developed by DHS and related testing we performed during this evaluation. The overall maturity level for FCA's contingency program 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,
- Identification of mission essential functions,
- An alternate recovery site to facilitate continuity of mission essential functions,
- Participation by senior executives and IT personnel during periodic continuity exercises,
- Self-evaluation of Agency performance following an annual continuity exercise, and
- An information system backup strategy that includes alternate storage facilities.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this evaluation was to independently assess FCA's information security program using the metrics identified by DHS and determine the effectiveness of FCA's information security program and practices.

We conducted the evaluation at FCA's headquarters in McLean, Virginia, from August 2019 through October 2019. The scope of this evaluation is limited to FCA's Agency-owned and contractor-operated information systems of record as of September 30, 2019.

We took the following steps to accomplish the objective:

- Identified and reviewed applicable laws, regulations, and guidance related to the objective,
- Identified and reviewed applicable internal FCA policies and procedures,
- Examined documentation relating to the Agency's information security program,
- Interviewed the CIO, Chief Information Security Officer, Chief Data Officer, personnel from OIT with significant responsibilities related to information security, and Personnel Security Officer,
- Updated our understanding from past FISMA evaluations,
- Reviewed prior evaluations and recommendations,
- Observed and tested a subset of security related activities performed by Agency personnel, and
- Judgmentally sampled supporting documentation, observations, and tests throughout the evaluation based on new and revised controls and risk to FCA operations. Because our samples were judgmental, the samples cannot be projected to the entire population.

This evaluation was performed in accordance with the CIGIE Quality Standards for Inspection and Evaluation. These standards require that we plan and perform the evaluation to obtain sufficient, competent, and relevant evidence that supports a reasonable basis for our findings, conclusions, and recommendations. We assessed internal controls and compliance with laws and regulations to the extent necessary to satisfy the objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our evaluation. We assessed the information and data collected during the evaluation and determined it was sufficiently reliable and valid for use in meeting the evaluation objective. We assessed the risk of fraud related to our evaluation objective while evaluating evidence. Overall, we believe the evidence obtained is sufficient to provide a reasonable basis for our findings and conclusions based on the evaluation objective.

REPORT FRAUD, WASTE, ABUSE, & MISMANAGEMENT:

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.