OFFICE OF

INSPECTOR GENERAL

Report of Audit

# Certification & Accreditation Process

A-09-01

**Tammy Rapp**
**Auditor-in-Charge**

**July 21, 2009**

FARM CREDIT ADMINISTRATION

**Farm Credit Administration**

Office of Inspector General
1501 Farm Credit Drive
McLean, Virginia 22102-5090

July 21, 2009

The Honorable Leland A. Strom
Chairman of the Board
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Chairman Strom:

The Office of Inspector General completed an audit of the certification and accreditation process used recently by the Farm Credit Administration to assess security controls and provide authorization to operate for its information technology infrastructure.

We determined that the certification and accreditation process was well planned and managed, and the process complied with the requirements and guidance provided by the Federal Information Security Management Act, the Office of Management & Budget, and the National Institute of Standards and Technology. We made suggestions throughout this audit, but did not make any formal recommendations.

We conducted the audit in accordance with *Government Auditing Standards* issued by the Comptroller General for audits of Federal organizations, programs, activities, and functions. We conducted fieldwork from December 2008 through June 2009. We provided a discussion draft report to management on June 18, 2009, and conducted an exit conference regarding the discussion draft report with the Chief Information Officer and Director of the Office of Management Services on July 7, 2009.

We appreciate the courtesies and professionalism extended to the audit staff. If you have any questions about this audit, I would be pleased to meet with you at your convenience.

Respectfully,

Carl A. Clinefelter

Carl A. Clinefelter
Inspector General

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The Office of Inspector General (OIG) performed an audit of the Farm Credit Administration's (FCA or Agency) certification and accreditation (C&A) process used on its information technology (IT) infrastructure. This was the first C&A performed at FCA by an internal certification agent, and FCA plans to use the same certification agent for future C&As. The objective of our audit was to evaluate the C&A process and determine if it complied with applicable laws, policy, and guidance and identify potential areas for improvement which can be applied to the next C&A.

The results of our audit revealed that FCA's C&A process was well planned and managed, and complied with the requirements and guidance provided by the Federal Information Security Management Act (FISMA), the Office of Management & Budget (OMB), and the National Institute of Standards and Technology (NIST). Our observations of the C&A process followed by the Agency disclosed the process contained the following elements:

- Proper and adequate planning;
- Security control testing executed in accordance with NIST guidance;
- No material gaps identified in security control testing;
- Appropriate reuse of previous assessments and evaluations;
- Adequate certification testing documentation, but could be improved (see page 7);
- Accreditation decision based on balancing mission and operations with security; and
- Effective continuous monitoring program.

Our audit did not reveal any significant deficiencies; therefore we did not make any formal recommendations. However, we did make suggestions to the certification agent throughout the audit that will further strengthen the C&A process. In addition, we informed the certification agent, information system owner, Information Security Specialist, and Chief Information Officer (CIO) of various new requirements from NIST and other changes currently being deliberated that will have an impact on FCA's IT security program.

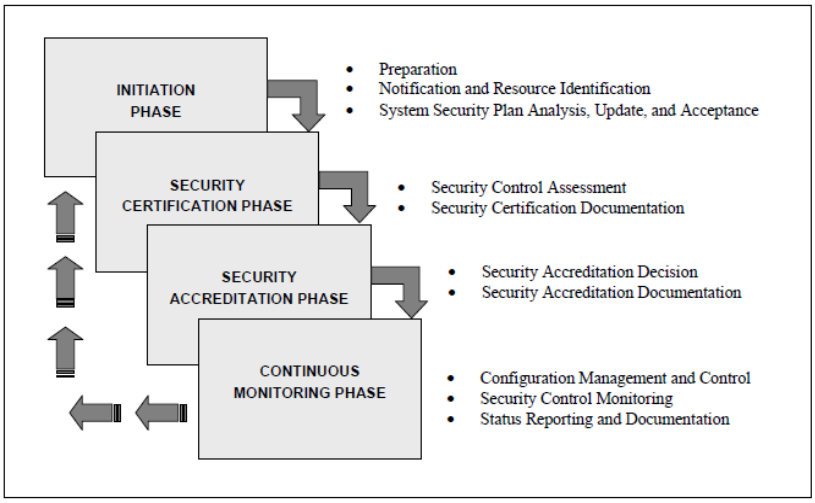
In OMB's annual reporting instructions for FISMA, it requests OIGs to provide a qualitative assessment of the C&A process. OMB's response categories include excellent, good, satisfactory, poor, and failing. In our professional judgment, we rated FCA's C&A process "good" based on the audit results described in this report.

# INTRODUCTION AND BACKGROUND

Agencies are required to perform a C&A of information systems every three years or when a major change occurs. Certification is the process of assessing the management, operational, and technical security controls of an information system to determine if they are implemented effectively. The certification results provide the authorizing official (AO) with an assessment of the effectiveness of security controls, identify weaknesses in the implementation of controls, and make recommendations for improvement where applicable. Accreditation is the authorization by an agency official to operate the system based on results of the certification and any residual risk remaining with the system.

FISMA was signed into law in December 2002 to strengthen the security of the Federal Government's information systems and develop minimum standards for agency systems. NIST was directed to develop standards, guidelines, and special publications (SP) to assist Federal agencies in complying with FISMA. FISMA and OMB policy require that Federal agencies comply with NIST standards and guidance.

NIST developed SP 800-37 to provide agencies with guidelines for the C&A of Federal information systems. In SP 800-37, NIST describes four phases and identifies tasks associated with each phase that comprise the C&A process. Each phase and task is described in more detail within the Observations section of this report.




Source: NIST SP 800-37 Figure 3.1

FISMA requires each respective OIG to conduct annual assessments of its agency's information security program and report the results to the OMB. OMB's annual FISMA reporting instructions require OIGs to assess agency C&A programs as part of their independent evaluation mandated by FISMA. The results of this audit will be used to fulfill that requirement.

In 2007, the FCA completed a C&A on two major applications. The security control assessment was performed by an independent contractor that included tests to validate that controls identified in the security plan were implemented and operating as intended. The general support system had a C&A in August 2005 and went through the process of recertification during 2008.

## OBJECTIVES

The objective of this audit was to evaluate FCA's C&A process and determine if the process complied with applicable laws, policy, and guidance and identify potential areas for improvement which can be applied to the next C&A.

## SCOPE AND METHODOLOGY

Our audit compared FCA's C&A process with the requirements of FISMA, OMB policy, and NIST guidance. The focus of our audit was the C&A performed on the infrastructure (previously named general support system) resulting in an interim authorization to operate in September 2008 and an unrestricted authorization to operate in January 2009. This audit concentrated on the initiation, certification, and accreditation phases presented in NIST SP 800-37.

We used NIST SP 800-37 and 800-53A as our primary benchmarks for evaluating FCA's C&A process. NIST SP 800-37 provides guidance on the C&A process, and NIST SP 800-53A provides security control assessment procedures for system controls.

In conducting this audit, we performed the following steps:

- Identified and reviewed FCA policies and procedures relating to C&A, including a sample of supporting policies and procedures;
- Identified key participants in the C&A process;
- Compared FCA's C&A process to NIST SP 800-37 and other related SPs;
- Reviewed the security plan, C&A assessment plan, previous independent assessments, security assessment report, and plan of action and milestones (POA&M);
- Examined documentation associated with the infrastructure C&A and compared to NIST standards and guidelines;
- Identified procedures performed and determined the appropriateness of tests performed by the certification agent based on NIST SP 800-53A; and
- Conducted interviews with the following key participants involved in the recent C&A:
    - CIO and AO,
    - Information system owner,
    - Certification agent,
    - Information Security Specialist, and
    - Other IT specialists.

This audit was performed at the FCA headquarters in McLean, Virginia, from December 2008 through June 2009, in accordance with generally accepted auditing standards for Federal audits.

# OBSERVATIONS

Procedures performed during our audit did not reveal any significant deficiencies in FCA's C&A process. Below you will find a summary of our observations for each C&A task.

## INITIATION PHASE

The initiation phase provides for the planning and preparation essential to the C&A process.

### Task 1: Preparation

"The objective of the preparation task is to prepare for security certification and accreditation by reviewing the system security plan and confirming that the contents of the plan are consistent with an initial assessment of risk.[1]"

We determined the information system owner adequately prepared for the C&A by reviewing the security plan and ensuring the security plan was consistent with the risk assessment. The security plan contained a description of the IT infrastructure, identified the security categorization, identified common controls, and a description of the security controls implemented.

FCA considered the risks to Agency operations, assets, individuals, and the Nation resulting from the operation of the infrastructure. The risk determination, including discussion of threats and vulnerabilities, was considered during the development of the security plan and the information system. Risks to information systems are continuously assessed and mitigated by evaluating security alerts, monitoring systems, and providing security related training and alerts.

### Task 2: Notification and Resource Identification

"The objective of the notification and resource identification task is to: (i) provide notification to all concerned agency officials as to the impending security certification and accreditation of the information system; (ii) determine the resources needed to carry out the effort; and (iii) prepare a plan of execution for the certification and accreditation activities indicating the proposed schedule and key milestones.[2]"

All appropriate Agency officials, including the AO, information system owner, Information Security Specialist, and certification agent, were aware of the impending security C&A for the IT infrastructure.

[1] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004, p.27
[2] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004, p.31

The individual selected as the certification agent is a FCA employee that reports directly to the AO. The organization chart and position descriptions were reviewed to identify potential independence issues. Although the certification agent does not report to the information system owner, there was a potential conflict in the area of contingency planning because the certification agent is also the continuity manager for FCA's Continuity of Operations Program (COOP) and author of several COOP documents. Although there appeared to be an independence issue, there were a couple of mitigating factors. First, the certification agent does not have any authority regarding the IT disaster recovery plan. Second, an external representative performed an independent evaluation of FCA's continuity program during the government-wide continuity exercise. Based on these mitigating factors, we determined there is not a substantive concern regarding the certification agent's independence.

The certification agent was provided with the resources necessary to conduct the C&A including specialized training, technical reference materials, documentation from previous assessments, NIST guidance, and access to key personnel and IT specialists. We made the following suggestion to the CIO:

- Provide the certification agent with additional technical training specific to FCA's infrastructure.

The certification agent developed an assessment plan based on key NIST guidance. The certification agent and AO had a clear understanding of the required timing of key C&A activities including the completion date. However, in the future, the certification agent should document the proposed schedule with key milestones and resources required in the assessment plan.

## Task 3: System Security Plan Analysis, Update, and Acceptance

"The objective of the security plan analysis, update, and acceptance task is to (i) perform an independent review of the FIPS 199 security categorization; (ii) obtain an independent analysis of the system security plan; (iii) update the system security plan as needed based on the results of the independent analysis; and (iv) obtain acceptance of the system security plan by the authorizing official and senior agency information security officer prior to conducting an assessment of the security controls in the information system.[3]"

The certification agent reviewed the security plan and ensured it was appropriately categorized and identified security controls that meet the security requirements for the system. The certification agent reviewed Federal Information Processing Standards Publication (FIPS) 199 and concurred with the information system owner's assessment resulting in a Moderate categorization based on confidentiality, integrity, and availability requirements for the system. FCA lowered its FIPS 199 ranking from high to moderate for

[3] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, p.33

the general support system, and we concurred with these ratings in 2007. There have been no changes since then that would necessitate a change in the security categorization ranking.

The comparison of the IT infrastructure security plan to the NIST SP 800-53A moderate baseline revealed that FCA included all the relative controls and tailored their security plan with a few additional high level controls. The IT infrastructure security plan provided an overview of the security requirements for the infrastructure, described specific controls, and delineated responsibilities for each control. The security plan also referenced related policies and procedures supporting individual controls. During the OIG's 2008 FISMA evaluation, we determined that the IT infrastructure security plan was closely aligned with the requirements of NIST SP 800-18.

The security plan was continuously updated throughout the certification process. To ensure all agreed modifications were made to the security plan, the certification agent verified the changes were incorporated in the resulting plan.

The CIO and information system owner agreed that the set of security controls proposed in the security plan meet the security requirements for the system.

## SECURITY CERTIFICATION PHASE

The purpose of the security certification phase is to determine whether security controls are implemented correctly, operating as intended, and meeting the security requirements of the system. The results of the certification provide the AO with the necessary information to determine if the residual risk of operating the system is at an acceptable level.

### Task 4: Security Control Assessment

"The objective of the security control assessment task is to (i) prepare for the assessment of the security controls in the information system; (ii) conduct the assessment of the security controls; and (iii) document the results of the assessment.[4]"

The certification agent properly planned for the security control assessment. Using NIST SP 800-53A as a guide, the certification agent developed a plan and conducted an assessment of the security controls outlined in the security plan for a moderate impact system.

The certification agent used a risk-based approach to determine the depth of assessment procedures and touched on every control contained in the security plan. The assessment was based on interviews, policy and procedure review, document examination, testing, and reliance on a previous independent network security assessment to determine if the security controls were implemented correctly, operating as intended, and providing the desired level

[4] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, p.35

of security for the system. The assessment procedures performed were closely aligned with NIST SP 800-53A.

The results of the assessment were adequately documented in a final report to the information system owner and AO including a worksheet that documented test procedures and results for each control. Although the documentation was adequate, we made suggestions throughout the audit to the certification agent that will improve future assessments. Our suggestions were well received and implemented immediately where possible. Below are some examples where we made a suggestion that will improve future documentation:

- When reviewing policies and procedures, include the published date of the documents reviewed and ensure they are current and updated; and
- Where specific tests are performed, document who did the test, when the test was performed, what tools were used, expected test results, actual test results, and supporting documentation (e.g., access control list, sample page of reports, screen shots, etc.).

## Task 5: Security Certification Documentation

"The objective of the security certification documentation task is to (i) provide the certification findings and recommendations to the information system owner; (ii) update the system security plan as needed; (iii) prepare the plan of action and milestones; and (iv) assemble the accreditation package.[5]"

The certification agent provided the information system owner with findings throughout the C&A process. The information system owner took immediate corrective action to resolve any findings, and the certification agent subsequently verified the corrective action resulting in no POA&M items. The system security plan was also updated as necessary throughout the C&A process and verified by the certification agent.

The final accreditation package contained an Executive Summary, Final IT Security Test & Evaluation (ST&E) Report including documented test procedures and results, and an updated system security plan. The certification agent recommended to the AO that an Authorization to Operate be granted for FCA's infrastructure as a result of her assessment of the management, operational, and technical security controls contained in the system security plan. The certification agent determined that the controls assessed in the system security plan were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

[5] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, p.38

## SECURITY ACCREDITATION PHASE

During the accreditation phase, the AO will determine if vulnerabilities remaining in the system after implementing the controls identified in the security plan represent an acceptable level of risk to agency operations, assets, and individuals. The AO's risk determination results in a formal decision of whether the system should be authorized to operate.

### Task 6: Security Accreditation Decision

"The objective of the security accreditation decision task is to (i) determine the risk to agency operations, agency assets, or individuals; and (ii) determine if the agency-level risk is acceptable.[6]"

The AO issued an "interim authorization" for the infrastructure to operate in September 2008. This interim authorization was issued as the previous authorization to operate was at the end of its lifecycle. The AO did not want to issue an unrestricted authorization to operate without the completion of thorough certification testing. In order to fulfill its mission, FCA needed to continue operating the system until testing was complete so the AO signed an "interim authorization."

In January 2009, the AO issued the final Authorization to Operate upon completion of certification testing, discussions with the certification agent, information system owner, Information Security Specialist, and review of the ST&E documentation. The accreditation decision was informed and based on Agency risk. The AO was intentional about balancing the mission and operational needs of the Agency without compromising security requirements.

### Task 7: Security Accreditation Documentation

"The objective of the security accreditation documentation task is to (i) transmit the final security accreditation package to the appropriate individuals and organizations; and (ii) update the system security plan with the latest information from the accreditation decision.[7]"

The final security accreditation package contained the updated and approved security plan, security assessment report, and authorization to operate. Due to the sensitivity of information contained within the C&A package, it was appropriately safeguarded with limited distribution. In lieu of the detailed security accreditation package, senior officials were provided with a characterization of its contents.

[6] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004, p.40
[7] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004, p.27

## CONTINUOUS MONITORING PHASE

The purpose of this phase is to ensure continuous monitoring and oversight of information systems is performed. An effective continuous monitoring program incorporates configuration management, security control monitoring, and status reporting.

### Task 8: Configuration Management and Control

"The objective of the configuration management and control task is to (i) document the proposed or actual changes to the information system; and (ii) determine the impact of proposed or actual changes on the security of the system.[8]"

FCA uses a disciplined approach to configuration management. Major changes are vetted through the information resources management planning process, and security is considered whenever proposed changes are made. In addition to maintaining an inventory of hardware and software, FCA documents configuration settings and exceptions to standard configurations. System updates, patches, and virus signatures are continuously updated. FCA uses an automated solution to periodically scan for known vulnerabilities, and significant deficiencies are immediately corrected when possible.

### Task 9: Security Control Monitoring

"The objective of the security control monitoring phase is to: (i) select an appropriate set of security controls in the information system to be monitored; and (ii) assess the designated controls using methods and procedures selected by the information system owner.[9]"

FCA uses a combination of real-time monitoring, self assessments, independent vulnerability assessments, and audits as part of its security control monitoring program. FCA has identified key controls and sensitive accounts that are part of its continuous monitoring strategy. A combination of automated and manual procedures is used to perform continuous monitoring. Over a 3-year cycle, FCA tests all controls contained in its security plan.

### Task 10: Status Reporting and Documentation

"The objective of the status reporting and documentation task is to: (i) update the system security plan to reflect the proposed or actual changes to the information system; (ii) update the plan of action and milestones based on the activities carried out during the continuous monitoring phase; and (iii) report the security status of the information system to the authorizing official and senior agency information security officer.[10]"

---

[8] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, p.43
[9] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, p.44
[10] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, p.45

FCA continuously updates the infrastructure security plan as needed and reviews it on an annual basis in conjunction with the information resource management planning cycle.

FCA's security philosophy is to correct identified deficiencies immediately, resulting in limited POA&M items. The POA&M is reviewed quarterly by the Information Security Specialist.

FCA is a small agency with effective communication. The CIO and Information Security Specialist are kept current and informed on issues involving security. The CIO has weekly meetings with Technology Managers and the Information Security Specialist. The CIO, Information Security Specialist, and other key IT Specialists have smart phones providing access 24 hours a day, every day of the week.

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| Agency | Farm Credit Administration |
| AO | authorizing official |
| C&A | certification and accreditation |
| CIO | Chief Information Officer and authorizing official |
| COOP | Continuity of Operations Program |
| FCA | Farm Credit Administration |
| FIPS | Federal Information Processing Standards Publications |
| FISMA | Federal Information Security Management Act |
| IT | information technology |
| NIST | National Institute of Standards and Technology |
| OIG | Farm Credit Administration's Office of Inspector General |
| OMB | Office of Management & Budget |
| POA&M | plan of action and milestones |
| SP | special publication |
| ST&E | security test & evaluation |

# R E P O R T

Fraud | Waste | Abuse | Mismanagement


FARM CREDIT ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

- Phone: Toll Free (800) 437-7322; (703) 883-4316
- Fax: (703) 883-4059
- E-mail: fca-ig-hotline@rcn.com
- Mail: Farm Credit Administration
  Office of Inspector General
  1501 Farm Credit Drive
  McLean, VA 22102-5090