Standard Operating Procedure

IT System Certification & Accreditation Process For FIPS 199 Low Systems

ITS-SOP-0031C
Effective Date: 20080707
Expiration Date: 20110707
Responsible Office: Office of the Chief Information Officer

Document Change and Review History

Version Number	Summary of Changes	Changes Made/Reviewed By	Date
1.0 (B)	Process adjustment and formatting	S. Hunt	2/27/08
1.1 (C)	Process adjustment and formatting	S. Hunt	3/1/08
1.2 (C)	Edit for structure and formatting	T. Fryer	4/1/08
1.3 (C)	Process adjustment and formatting	S. Hunt	4/9/08
1.4 (C)	Process adjustment	S. Hunt	6/17/08

Table of Contents

1.0 Introduction 1
2.0 Certification and Accreditation Web Portal 1
3.0 Process Step Format & Acronyms 1
4.0 Role-Based Email Addresses 1
5.0 Certification & Accreditation Process 2
5.1 Phase I - Security Categorization & SSP Documentation 2
5.2 Phase II - IT Security Documentation Preliminary Review 6
5.3 Phase III – Certification 8
5.4 Phase IV - Accreditation Package 8
6.0 Approval 10
Appendix A: C&A Web Portal 11
Appendix B: Roles and Responsibilities 12

1.0 Introduction

The NASA Certification and Accreditation (C&A) program follows OMB and National Institute of Standards and Technology (NIST) standards and guidelines pertaining to information technology systems security. These document sets outlines the general process for achieving certification and accreditation of Federal Government computer systems. This SOP defines the specific NASA procedure and timeline for C&A of NASA computer systems in accordance with the OMB and NIST guidance.

2.0 Certification and Accreditation Web Portal

The most recent version of all forms, checklists, and documentation referenced in this SOP can be located via the "Certification and Accreditation" section of the NASA "Office of the Chief Information Officer" (OCIO) website:

http://insidenasa.nasa.gov/ocio/security/CA/index.html

You are encouraged to visit the C&A Web Portal regularly to keep up-to-date with the NASA C&A program, policies, procedures, guidance, supporting forms, and NIST documents.

3.0 Process Step Format & Acronyms

Acronyms for key individuals within the NASA certification and accreditation process are provided below.

Step #: [role associated with the process step]; details of the process step

AO	- **A**uthorizing **O**fficial
CA	- **C**ertification **A**gent
CAO	- **C**ertification and **A**ccreditation **O**fficial
CAPM	- **C**ertification and **A**ccreditation **P**rogram **M**anager
ISO	- **I**nformation **S**ystem **O**wner
ITSM	- **I**nformation **T**echnology **S**ecurity **M**anager
NSSPR	- **N**ASA **S**ystem **S**ecurity **P**lan **R**epository (currently RMS)
OC	- NSSPR **O**perations **C**enter
OCSO	- **O**rganizational **C**omputer **S**ecurity **O**fficial
PCAO	- **P**rincipal **C**ertification and **A**ccreditation **O**fficial
PO	- **P**ackage **O**wner

Figure 1 – Acronym Key

4.0 Role-Based Email Addresses

NSSPR Operational Support – CASupport@Nasa.Gov

5.0 Certification & Accreditation Process

5.1 Phase I - Security Categorization & SSP Documentation

The Security Categorization & SSP Documentation phase addresses those actions performed by the Information System Owner (ISO), Organizational Computer Security Official (OCSO), IT Security Manager (ITSM), and Certification & Accreditation Official (CAO) that categorize and generate the IT security documentation required for certification and accreditation.

Step 1.1: **[ISO/OCSO/ITSM]**

The ISO for the system to be certified and accredited, with guidance and direction from their local OCSO and ITSM, will derive the system security categorization per ITS-SOP-0019 – "Procedure for the FIPS-199 Categorization of IT Systems", Federal Information Processing Standard (FIPS) 199, and NIST SP 800-60. Document the resulting security categorization in the "SYSTEM SECURITY CATEGORIZATION RECORD" located via the C&A Web Portal.

Guideline: The ISO should work with application owners and/or information owners to ensure that all information on the system is identified and incorporated when deriving the system security category.

Step 1.2: **[ISO]**

The ISO for the system to be certified will fill out the "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form located via the C&A Web Portal.

Step 1.3: **[ISO]**

The ISO will E-mail the completed "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form, the "SYSTEM SECURITY CATEGORIZATION RECORD", and any supporting documentation to the local Center CAO.

Guideline: When submitting the above forms to the CAO use the following naming conventions:

1) Name the "Subject" field of the E-mail using the following format:

   Format: **CAOVR-SC:** ***<ITSSP name>***

   Example: **CAOVR-SC: Code A Windows Systems**

2) Name the "SYSTEM SECURITY CATEGORIZATION RECORD" file using the following format:

   Format: **SCR** ***<ITSSP name >***

   Example: **SCR Code A Windows Systems**

3) Name the "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" file using the following format:

   Format: **CAOVR-SC** ***<ITSSP name>***

   Example: **CAOVR-SC Code A Windows Systems**

Step 1.4: **[CAO/ITSM/OCSO/ISO/AO]**

The CAO, in coordination with the ITSM and/or OCSO, will review the submitted security categorization documentation and issue a "concur" or "non-concur" response to the ISO by completing and signing the "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION".

If **Concur** response confirms the categorization and allows for the system to continue with the C&A process. Go to Step 1.5.

If **Non-Concur** response will be accompanied with a non-concur justification. The ISO then has the option to:

- Re-categorize the system based on the CAO recommendation or
- Arrange a meeting with the system Authorizing Official (AO), the CAO, OCSO, and the ITSM to determine a resolution. The certification cannot proceed until a resolution is accepted by the AO and the CAO.

Step 1.5: **[CAO/ISO/ITSM]**

- The CAO returns the approved "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form, along with any supporting documentation, to the ISO.
- The ITSM is copied on this response so that they are notified that a new System Security Plan (SSP) certification package has been approved for generation in the NASA System Security Plan Repository (NSSPR).
- Once the certification package has been generated the ISO uploads the approved "REQUEST FOR CAO VALIDATION OF SECURITY CATEGORIZATION" form and the "SYSTEM SECURITY CATEGORIZATION RECORD" to the NSSPR as artifacts of the certification package.

Step 1.6: **[ISO/ITSM]**

The ISO will identify users who require access to the NSSPR. The ISO will apply for NSSPR accounts by completing the appropriate NSSPR ACCESS REQUEST form, located via the C&A Web Portal, and submitting it to the local Center ITSM.

Guideline: All users for whom an account is requested *must* have a current PKI certificate.

Step 1.7: **[ITSM/OC]**

ITSM will review and approve or decline account creation.

If **Approved** ITSM will email or fax the account information to the Operations Center (OC) for the NSSPR.

If **Declined** ITSM will provide justification for rejection and return the form to the requester via email or fax. The requester may resubmit the account request after addressing the ITSM's concerns.

Step 1.8: **[OC]**

The OC will create the accounts and send an encrypted email to the new users with their username and password within one (1) week of receipt of the NSSPR ACCESS REQUEST Form.

Step 1.9: **[ITSM]**

The ITSM will generate the SSP certification package within the NSSPR. Note that the ITSM can delegate this portion of the process to the ISO, OCSO, a local C&A plan writing team, or anyone else they deem appropriate for this role.

Requirement: When generating the SSP certification package the following naming convention is a NASA procedural requirement:

Format: ***<ITS-SOP-0007 System Designation> <System Name>***

Example: **AR-999-L-ARC-0103 Code A Windows Systems**

Step 1.10: **[ISO/ITSM/OCSO]**

The ISO, with guidance and direction from their local ITSM via their OCSO, populates the System Security Plan (SSP) certification package within the NSSPR.

Guideline: Once an SSP certification package is created, the ISO will continue populating it using the template, formats, requirements, etc. that were in effect at the time the certification package was created. Version numbers of templates or requirements used should be clearly noted where relevant in the SSP certification package. If a template or requirements change during this process, compliance with new requirements or formats should be noted as a required action in the system's Plan of Actions and Milestones (POA&M), with a completion date of no later than one year from the date of the system's new Authorization to Operate.

Step 1.11: **[ISO/OCSO]**

The ISO, in coordination with the OCSO, uses the "CERTIFICATION PACKAGE REVIEW CHECKLIST" (CPRC), downloaded via the C&A Web Portal, to verify that the package is ready for Certification Review. If any significant issues exist they must be corrected prior to continuing the Certification Review process. Minor issues can be documented in the Checklist with recommendations for correction. The "CERTIFICATION PACKAGE REVIEW CHECKLIST" is then uploaded to the NSSPR as an artifact of the certification package.

Guideline: Prior to uploading the above form to the NSSPR name the file using the following naming conventions:

Format: **CPRC *<ITS-SOP-0007 System Designation> <System Name>***

Example: **CPRC AR-999-L-ARC-0103 Code A Windows Systems**

Step 1.12: **[ISO/CAO]**

The ISO notifies the CAO via E-mail that the package is ready for Certification Review.

Guideline: When submitting the above notification to the CAO use the following naming convention:

Name the "Subject" field of the E-mail using the following format:

Format: **CPRC: *<ITS-SOP-0007 System Designation> <System Name>***

Example: **CPRC: AR-999-L-ARC-0103 Code A Windows Systems**

5.2 Phase II - IT Security Documentation Preliminary Review

The IT SSP Preliminary Review phase addresses those actions performed by the CAO associated with reviewing the SSP certification package to ensure that all required IT Security documentation has been generated properly and is complete.

Step 2.1: **[CAO]**

The CAO logs into the NSSPR and, using the "CERTIFICATION PACKAGE REVIEW CHECKLIST" submitted by the ISO, verifies that the certification package meets requirements. The CAO documents any variances in the "Certification Review Variance Dispositioning" section of the CPRC.

Step 2.2: **[CAO]**

Is the Certification Package acceptable for continued processing?

If **Yes** - go to Step 3.1

If **No** - go to Step 2.3

Guideline: At this point in the process, if time constraints are tight towards meeting ATO deadlines, the remainder of Phase 2.0 can be performed in parallel with Phases 3.0 and 4.0. In cases such as this only "significant variances" should prevent the initiation of the "Independent Certification Contract" in Phase 3.0 and the subsequent "SSP Review" process in Phase 4.0. Being that the SSP Review phase primarily concerns an initial review of the SP 800-53 controls suite a gross lack of proper documentation relative to the control suite would be an example of a significant variance that could prevent continued processing.

Resolution of other identified variances contained within the larger scope of the SSP, as documented in the "CERTIFICATION PACKAGE REVIEW CHECKLIST", should be worked concurrently with Phases 3.0 and 4.0. The goal is the generation of an SSP that is as compliant as possible with policy, procedures, standards, and guidelines, prior to the IDCCT visiting the site as outlined below in Phase 6.0.

Step 2.3: **[CAO/ISO]**

The CAO notifies the ISO that the Certification Package is not acceptable for continued certification processing and instructs the ISO to correct variances per instruction the CAO has documented in the "CERTIFICATION PACKAGE REVIEW CHECKLIST".

Step 2.4: **[ISO]**

ISO corrects variances per instructions from CAO, completes the "Certification Review Variance Dispositioning" section of the CPRC, and returns it to the CAO.

Step 2.5: **[ISO/CAO]**

The ISO notifies the CAO that the variances have been corrected and the package is ready to resume the Certification Review process.

Step 2.6: **[CAO]**

The CAO verifies that the variances have been corrected. Is the Certification Package acceptable for continued processing?

If **Yes** - go to Step 3.1

If **No** - go to Step 2.3

If No agreement can be reached go to Step 2.7

Step 2.7: **[ISO/CAO/ITSM/AO]**

In the event that an agreement cannot be reached between the ISO and the CAO concerning the acceptability of the Certification Package, the ISO will arrange a meeting between the ISO, CAO, ITSM, and AO (at a minimum) to determine how to proceed. The AO is required to make a decision about whether to continue the certification process with or without addressing the CAO concerns.

- If AO chooses to not address CAO concerns, the CAO will document the decision, receive a signature of the decision from the AO on the CPRC, and upload the documented decision and CPRC as artifacts to the SSP certification package – proceed to Step 3.1
- If AO chooses to address CAO concerns – go to Step 2.3.

5.3 Phase III – Certification

Referring to the "Security Certification Phase" of NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems", note that for systems with a security categorization of Low the Certification Phase consists of a "Self-Assessment" of the information systems security controls. In alignment with this, the CAO approved CERTIFICATION PACKAGE REVIEW CHECKLIST is deemed synonymous with the Security Assessment Report that is the core deliverable for the Certification Phase, as it requires both the SO and CAO to review all documentation pertinent to validating the security posture of the system.

The SO should insure, prior to submitting the CERTIFICATION PACKAGE REVIEW CHECKLIST to the CAO for review, that all standards, guidelines, procedures, and processes reflected in the documents referenced in the checklist have indeed been implemented and fulfilled as stated.

5.4 Phase IV - Accreditation Package

The accreditation package phase includes creation of the accreditation package and submission of the package to the AO.

Step 4.1: **[ISO]**

The ISO will create an accreditation package for the AO. The accreditation package includes (at a minimum):

- Executive summary to the AO:
  - Short summary of the findings
  - Actions taken to address findings
  - Risks AO is accepting
  - ISO's recommendation for ATO, IATO, or DATO
- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Plan of Actions and Milestones (POA&M)

Guideline: For systems with a "Low" security categorization the CAO approved "Certification Package Review Checklist" serves as the SAR.

Step 4.2: **[AO/ISO]**

The AO will review the certification package, make an accreditation decision (see NPR 2810.1A, section 14.4.3), and complete the Authorization to Operate (ATO), Interim ATO (IATO), or Denial of ATO (DATO) form available via the C&A Web Portal. The AO will then forward the accreditation decision to the ISO. Is the AO decision to operate?

If **Yes** - go to step 4.4

If **No** - go to step 4.3

Guideline: The AO may seek consultation with the ITSM, CAO, OCSO or others tangential to the C&A process, prior to making a final decision towards accreditation of the system. If so, the AO should be provided with pertinent information that details the residual risk to NASA missions, assets, or personnel associated with operation of the system.

Step 4.3: **[ISO]**

The ISO will input the decision letter into NSSPR and cease operation of the system.

Step 4.4: **[ISO]**

The ISO will input the decision letter into NSSPR and begin or continue operation of the system.

Certification and Accreditation Process Complete

6.0 Approval

Jerry L. Davis
Deputy CIO IT Security
Senior Agency Information Security Officer

7 Jul 08
Date

Appendix A: C&A Web Portal

Please visit the "Certification and Accreditation" section of the NASA "Office of the Chief Information Officer" (OCIO) website for all documents referenced in this SOP. The C&A section can be accessed directly via the following link:

http://insidenasa.nasa.gov/ocio/security/CA/index.html

Appendix B: Roles and Responsibilities

OCIO Responsibilities:

OCIO is responsible for developing NASA C&A policies and procedures for unclassified IT systems. In addition OCIO has responsibility for the implementation, tracking, and enforcement of Federal and NASA C&A requirements. These responsibilities include the following:

- **NASA C&A Program Management**:
  The NASA C&A Program Manager is responsible for implementing and managing the NASA C&A program, as described below, with the help of the NASA Principal Certification & Accreditation Official (PCAO), Center Certification & Accreditation Officials (CAO), Center ITSM's, and the Independent Certification Project Manager (ICPM).

- **Agency Principal Certification & Accreditation Official (PCAO):**

  - Function as lead and POC for all Center CAO's.
  - Liaison between Agency C & A Program Manager and Center CAO's.
  - Execute wide variety of tasks as identified and assigned by the Program Manager for C&A.
  - Facilitates development of Agency C&A policies and procedures.
  - Lead weekly Agency C & A telecoms that address C&A related topics, issues, and concerns.
  - Manage Agency E-forms development, implementation, & maintenance integral to C&A
  - Facilitates development and management of Agency C&A web site hosted by OCIO.
  - Attend and facilitate C&A related tracts for Agency ITSM Conferences.
  - Directly or indirectly resolves C&A related issues and concerns as brought forth from various points throughout the Agency via CAO's and others tangential to the C&A process.

- **Center Certification & Accreditation Official (CAO):**
  This group is coordinated by the NASA Principal CAO who performs this function on behalf of OCIO.

  - Management, facilitation, and tracking of all certifications and accreditations for their Center.
  - Primary point of contact for all local C&A-related questions, issues, and concerns.
  - Primary POC for all local RMS content change requests.
  - Facilitate training and awareness relative to C&A requirements, procedures, and processes.
  - Review & Validate system security categorizations.
  - Certification cost review to assure system components are in-line with independent certification cost estimates.
  - Facilitation, coordination, and POC for all independent system certifications at their Center.
  - Facilitation and coordination of communication between independent certifiers, independent certification contract, and SO's.
  - Verification of certification package including review of all Center SSP's and associated documentation for concurrence with Agency, NIST, OMB and other Federal Policies, Procedures, Standards, and Guidelines.
  - Document variances and recommended corrective measure in the Certification Package Review Checklist.
  - Facilitate generation of Plan of Action and Milestones (POA&M) in coordination with Center ITSM, SO, and AO.
  - Tracking and Review of the annual assessments of Continuous Monitoring controls.
  - Facilitate External Systems reviews and assessments.
  - Monthly (or more frequent) coordination and status meetings with Center ITSM and CIO.

- **CIO / ITSM:**
  Each Center CIO, ITSM, and CAO should work closely together to ensure questions and concerns are resolved early in the C&A process. Center CIO's, through their ITSM's, are responsible for the following:

  - Reviewing C&A documentation and decisions.
  - Tracking the progress of systems in meeting C&A requirements.
  - Tracking systems' Plans of Actions and Milestones (POA&M).
  - Enforcing C&A requirements as necessary.

- **Managing the NASA Independent Certification Contract**

- **Development and Management of C&A related SOPs**

- **Managing the "Certification and Accreditation" section of the NASA "Office of the Chief Information Officer" (OCIO) website.**

- **Managing the "NASA System Security Plan Repository" (NSSPR)**

- **Managing the Agency POA&M process and tool(s)**

- **C&A of OAIT, Multi-Program funded systems, and OCIO/Center systems** – As NASA organizations, NASA OCIO and each Center OCIO has the responsibility of meeting C&A requirements for the relevant OAIT, Multi-Program funded systems, and Center information systems.