Information Assurance Procedures

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545maq_060106_cd44

Information System Security
Information Assurance Procedures
For System Owners and Information System Security Officers, Certification Teams, and Designated Approving Authorities (DAAs)

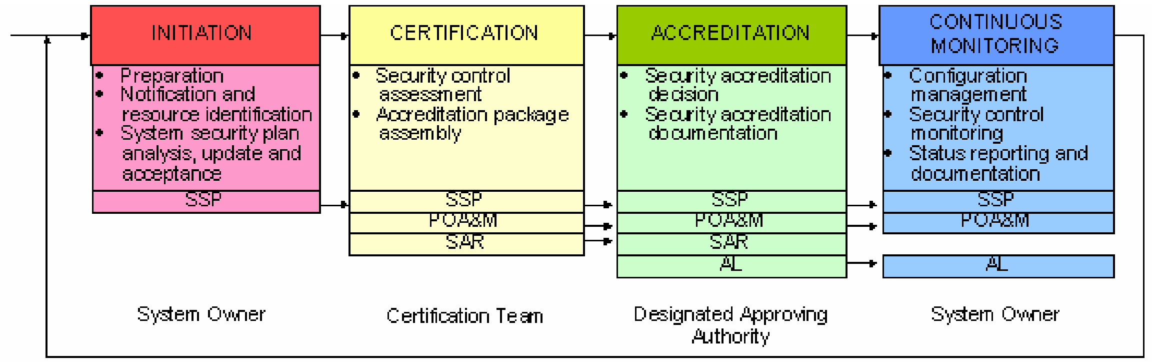
1. Introduction

This document defines the process for certification and accreditation of USAID information systems.

2. Certification and Accreditation (C&A)

Certification and accreditation is the process by which an information system is assessed to determine that the system meets the security requirements for the mission function and the sensitivity of information handled. A certification and accreditation must be performed once development of the information is complete. Certificate and Accreditation are performed throughout the information system's life cycle; they also support the risk management process.

The following chart provides an overview of the C&A process. The process consists of four phases: Initiation, Certification, Accreditation, and Continuous Monitoring. Each of the four phases is broken down into the high-level tasks and supporting documents – System Security Plan (SSP); Plan of Action & Milestones (POA&M); Security Agreement Report (SAR); Accreditation Letter (AL) – that are required for that phase.


INITIATION
• Preparation
• Notification and resource identification
• System security plan analysis, update and acceptance
SSP
System Owner
CERTIFICATION
• Security control assessment
• Accreditation package assembly
SSP
POA&M
SAR
Certification Team
ACCREDITATION
• Security accreditation decision
• Security accreditation documentation
SSP
POA&M
SAR
AL
Designated Approving Authority
CONTINUOUS MONITORING
• Configuration management
• Security control monitoring
• Status reporting and documentation
SSP
POA&M
AL
System Owner

The above graphic shows a four-phase flowchart that describes the responsibilities of the System Owner, Certification Team and the Designated Approving Authority for each phase. The phases are color coded as follows; Initiation – red, Certification – Yellow, Accreditation – Green, and Continuous Monitoring – Blue.

(1) **Initiation** is the phase in which the System Owner prepares for certification activities. This includes preparing the required documentation, notifying the Agency officials that the system is ready for C&A, and ensuring that the SSP is up-to-date.

(2) **Certification** is the phase in which a certification team performs a comprehensive evaluation of the information system's technical and non-technical security features and other safeguards to establish the extent to which the information system meets the specified security requirements. When the information system passes certification, the System Owner assembles the accreditation package. The accreditation package includes the SAR, the updated SSP, and the POA&M.

(3) **Accreditation** is the phase in which the System Owner submits the accreditation package to a Designated Approving Authority (DAA), who decides whether or not the system will be authorized to operate. The DAA issues the decision in a letter, and transmits the decision letter and the accreditation package back to the System Owner. The System Owner either deploys the information system to production or further modifies it as needed to receive an authorization to operate. **Note: USAID deviates from NIST guidance in that the System Owner may also be the DAA.**

(4) **Continuous monitoring** is the phase that occurs after the information system receives authorization to operate, in which the System Owner monitors and tracks changes to the information system's security controls over time. Reaccreditation must be performed when a significant change occurs to the information system or every three years. The system may require recertification if a significant change requires testing by the certification team. Reaccreditation may also be required if a new authorizing official is assigned to the information system.

The certification and accreditation process for System Administrators, System Owners, ISSOs, Certification Team, and DAAs is depicted in the flow chart in Section 3. The first phase of Certification and Accreditation, **Initiation**, is described in the next section.

2.1 Initiation

The purpose of the initiation phase is to confirm that security requirements for the information system are documented and that the CISO and DAA accept them before certification begins. The majority of the information needed was gathered during the initial risk assessment of the information system.

During the initiation phase, the System Owner reviews the SSP to ensure that it is complete and up-to-date. The SSP provides an overview of the security requirements for the information system and describes the security controls in place to meet those requirements. The SSP contents vary according to the security categorization of the system.

Security categorizations are defined according to the level of effort required for certification. There are three security categorizations, which are defined as follows:

Level of Effort	Low	Medium	High
Level of Effort Activities	Baseline Security Requirements (BLSRs) as checklist	• BLSRs as checklist • Additional system-specific requirements	• BLSRs as checklist • Additional system-specific requirements • System Testing & Evaluation (ST&E) • Vulnerability scanning • Penetration testing

This table defines the three security categorizations and the level of effort based on them.

Baseline security requirements refer to the minimum security requirements recommended for an information system based on the system's security categorization in accordance with Federal Information Processing Standard (FIPS) Publication 199.

The following table lists the SSP sections required for systems in each security categorization.

SSP Section	Low	Medium	High
Application/System Identification	X	X	X
Management Controls	X	X	X
Operational Controls	X	X	X
Technical Controls	X	X	X
Acronym List	X	X	X
Definitions	X	X	X
References	X	X	X
Security Requirements Compliance Matrix (SRCM)	X	X	X
Minimum Security Checklist	X	X	X
Formal Security Testing and Evaluation Plan and Procedures	N/A	As Needed	X
Certification Results (test results)	X	X	X
Risk Assessment and POA&M	X	X	X
Certification Authority Recommendations	X	X	X
System Security Policy	N/A	As Needed	X
System Rules of Behavior	N/A	X	X
Security Operating Procedures	N/A	As Needed	X
Business Continuity Plan (BCP)	N/A	As Needed	X
Disaster Recovery Plan (DRP)	N/A	As Needed	X
Security Awareness and Training Plan	N/A	As Needed	X
Personnel Controls and Technical Security Controls Certification Statement	N/A	X	X
Incident Response Plan	N/A	X	X
System Interconnection Agreements	X	X	X
System Documentation	X	X	X
Accreditation Documentation and Accreditation Statement	X	X	X
Memorandums of Understanding	X	X	X
Configuration Management Plan	X	X	X
Privacy Impact Assessment	X	X	X
Document History	X	X	X

This table lists the required SSP sections for systems in each security categorization.

For a sample System Security Plan, see the **System Security Plan Template**.

When the initiation phase concludes, then the certification phase begins.

2.2 Certification

In the certification phase, the certification team evaluates the information system to determine if the security requirements have been met, and identifies any deficiencies or vulnerabilities. The System Owner is responsible for correcting deficiencies/vulnerabilities that are severe enough to prevent system operation from being approved.

When the certification team completes the evaluation, the System Owner assembles the security accreditation package. The security accreditation package includes:

- System Security Plan. The SSP must reflect the current system. If there are modifications to the system security controls as a result of the certification evaluation, then the System Owner must update the SSP to reflect these changes.

- Security Assessment Report. This is the certification team’s report of the security evaluation, and the extent to which the information system has met the security requirements.

- Plan of Action and Milestones. A description of measures implemented or planned to correct deficiencies and to reduce/eliminate vulnerabilities. The System Owner documents the deficiencies/vulnerabilities identified by the certification team. For deficiencies/vulnerabilities not severe enough to require immediate remediation, the System Owner documents corrective action planned for completion when the system receives an interim authorization to operate from the DAA.

When the certification phase concludes and the System Owner is ready to transmit the accreditation package to the DAA, the accreditation phase begins.

2.3 Accreditation

The purpose of the accreditation phase is to determine if the information system meets the security requirements sufficiently to be allowed to operate. The System Owner transmits the accreditation package to the DAA. When the DAA receives the security accreditation package, he or she makes a decision as to the status of the system. The DAA can issue one of three accreditation decisions:

- Authorization to Operate (ATO). The information system is allowed to operate without any limits or restrictions.

- Interim Authorization to Operate (IATO). The information system is allowed to operate for a limited period of time at a greater risk to USAID, while the errors are corrected.

- Denial of Authorization to Operate (DATO). The information system is not allowed to operate.

The DAA and CISO review the certification assessment results. If the DAA determines that the risk level is acceptable for operation, then the DAA issues an ATO for the information system. The System Owner can then deploy the information system to production.

If the DAA determines that the risk level is unacceptable, but that corrective action(s) should be undertaken, the DAA issues an IATO for the information system. Once the DAA issues an IATO, the System Owner may put the information system into production for a limited time. The System Owner must correct the remaining deficiencies/vulnerabilities through remediation exercises within the required timeframe. If remediation is completed within the required timeframe, then the System Owner resubmits the information system for accreditation; if, at the discretion of the DAA, the changes need to be reverified, then the information system will need to be recertified also. If remediation is not completed within the required timeframe, the information system will not receive an authorization to operate; the System Owner will need to modify, correct, or redesign the information system before submitting it for certification and accreditation again.

If the DAA determines that the risk level and planned corrective action(s) are unacceptable, the DAA issues a DATO for the information system. The System Owner will need to modify, correct or redesign the information system before submitting it for certification and accreditation again.

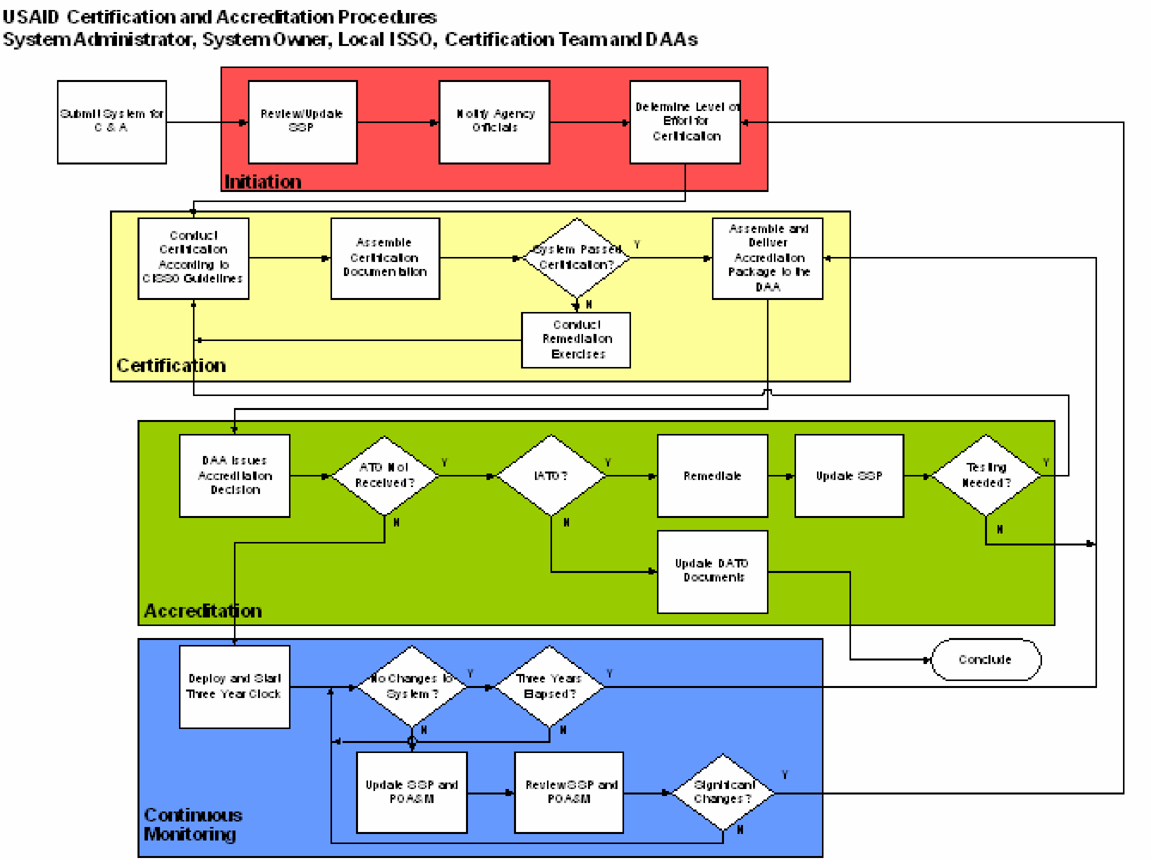
Once the DAA makes the accreditation decision, the DAA transmits the accreditation decision letter and the accreditation package back to the System Owner. The System Owner updates the SSP to reflect any changes in the information system resulting from the accreditation decision. If the information system received authorization to operate, then the continuous monitoring phase begins.

2.4 Continuous Monitoring

The purpose of the continuous monitoring phase is to provide oversight and monitoring of the security controls in the information system over time. During this phase, the System Owner tracks changes to the information system, using the established configuration management process, and monitors security controls. The System Owner updates the SSP and the POA&M to reflect any changes. When changes to the information system that impact the information system’s security occur, the System Owner must report those changes to the authorizing official and agency Information System Security Officer (CISO); the System Owner must then submit the information system for reaccreditation. The System Owner must submit the information system for reaccreditation every three years.

3. Certification and Accreditation Flow chart

The certification and accreditation process for System Administrators, System Owners, ISSOs, Certification Team, and DAAs is described in the following flow chart:


USAID Certification and Accreditation Procedures
System Administrator, System Owner, Local ISSO, Certification Team and DAAs
Submit System for C & A
Review/Update SSP
Notify Agency Officials
Determine Level of Effort for Certification
Initiation
Conduct Certification According to CISSO Guidelines
Assemble Certification Documentation
System Passed Certification?
Y
N
Assemble and Deliver Accreditation Package to the DAA
Conduct Remediation Exercises
Certification
DAA Issues Accreditation Decision
ATO Not Received?
Y
N
IATO?
Y
N
Remediate
Update SSP
Testing Needed?
Y
N
Update DATO Documents
Accreditation
Conclude
Deploy and Start Three Year Clock
No Changes to System?
Y
N
Three Years Elapsed?
Y
N
Update SSP and POA&M
Review SSP and POA&M
Significant Changes?
Y
N
Continuous Monitoring

This drawing shows the four phases involved in a C & A as described in this document. Each phase is color coded to correspond to the first chart found in this document.

4. References

Public Law 104-13, **Paperwork Reduction Act of 1995**.

Public Law 104-106, **National Defense Authorization Act for Fiscal Year 1996 see Section 2 Division E., Information Technology Management Reform Act of 1996**.

Public Law 107-347, **E-Government Act of 2002**.

FIPS PUB 199, **Standards for Security Categorization of Federal Information and Information Systems**, December 2003.

NIST SP 800-18, **Guide for Developing Security Plans for Information Systems**, December, 1998.

NIST SP 800-30, **Risk Management Guide for Information Technology Systems**, January 2002.

NIST SP 800-37, **Guide for the Security Certification and Accreditation of Federal Information Systems**, May 2004.

NIST SP 800-53, **Recommended Security Controls for Federal Information Systems** *DRAFT*.

NIST SP 800-59, **Guideline for Identifying an Information System as a National Security System**, August 2003.

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories Version 2.0, **Volume I**, **Volume II Appendixes**, June 2005. and

OMB Circular A-130, **Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources**, November 2000.

OMB Memorandum 02-01, **Guidance for Preparing and Submitting Plans of Action and Milestones**, October, 2001.