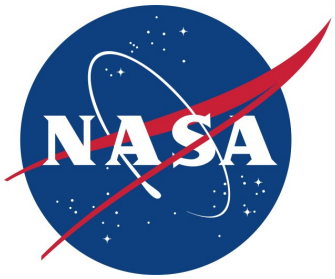

Standard Operating Procedure

Procedures for Submitting a NASA Agency Forest (NAF) Deviation Request and Transition Plan

EA-SOP-0003

Version Date: **July 30, 2008**
Effective Date: **August 1, 2008**
Expiration Date: **August 1, 2010**
Responsible Office: **OCIO, Chief Information Officer**

Revision Record

ITEM NO.	REVISION	DESCRIPTION	DATE
1	V.1.0	Initial Version	7/30/2008

Procedures for Submitting a NASA Agency Forest (NAF) Deviation Request and Transition Plan

Purpose

This document establishes the format and procedures for submitting a Deviation Request and Transition Plan for deviation from the prescribed NASA Agency Forest (NAF) architecture. The NAF architecture prescribes a single Active Directory (AD) forest for the Agency.

The Deviation Request and Transition Plan covers the following two major types of cases:

- Center AD installations not capable of being migrated
- NAF AD trust with a third party

The Deviation Request and Transition Plan differs from a waiver in that while the deviation process recognizes that certain Centers can not fully comply with NAF requirements, it does not provide a variance to the requirement to consolidate into the NAF. Instead this deviation process allows for deviations under specific circumstance and mandates a corresponding Deviation Transition plan that defines when the legacy AD forest will be consolidated into the NAF, or decommissioned**.**

Scope

This plan applies to all NASA implementations of Microsoft Active Directory that are in scope of the NASA Consolidation of Active Directory (NCAD) project. Nominally all Agency implementations of AD are in scope for NCAD with the specific exemptions of the Jet Propulsion Laboratory (JPL), Mission networks, and special cases such as Wind Tunnel networks.

Applicable Documents

- NPR 2810.1a, May 2006, “Security of Information Technology”
- OCIO Memo, January 31, 2006, “Review and Approval of Changes to Information Technology Baseline”
- NIST Special Publication 800-47, August 2002,
  Security Guide for Interconnecting Information Technology Systems
  http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf
- NIST Special Publication 800-100, October 2006,
  Information Security Handbook: A Guide for Managers
  http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
- NASA ITS-SOP-0033, July 2007,
  External System Identification and IT Security Requirements
  http://nodis-dms.gsfc.nasa.gov/restricted_directives/SOP_Docs/SOP_0033-_.pdf

Roles and Responsibilities

The following roles and responsibilities apply to this SOP:

- Author

  Follow the instruction of this document and the Deviation Request and Transition Plan template to make a deviation request.

- Center NCAD POC

  Review and provide concurrence/non-concurrence with the submitted request.

- Center CIO

  Review and provide concurrence/non-concurrence with the submitted request.

- NCAD Project Manager

  Review and provide concurrence/non-concurrence with the submitted request. Route through NASA OCIO. Coordinate follow-on action with the NAF team upon concurrence of the NASA CIO.

- NASA CIO

  Provide final concurrence/non-concurrence with the submitted request, and inform the NCAD Project Manager of the decision.

Process

The organization within the requesting Center will utilize the following procedures to create a NAF Deviation and Transition Plan:

- **Identify the applicable NAF deviation case.**

  The following cases have been identified and *may* be considered for eligibility to operate within the NAF architectural environment.

  Please review the applicability section for each of the following six (6) use cases in Appendix A. It is expected that all deviations requests should be able to be mapped to one of these cases.

Table 1 -- Deviation Case Summary

Case	Name (Deviation Case Type)
1	CRF where the CRF contains resources only
2	CRF where the CRF contains user accounts
3	Legacy Resource Forest (LRF) where the LRF contains resources only
4	Trust with External Entities where the external entity uses NAF user accounts
5	Retiring Resource Forest (RRF) where the RRF contains resources only
6	Retiring Forest (RF) where the RF contains user accounts

Note: When considering the phrase “contains user accounts” used in the description throughout these deviation cases, we recognize that AD requires the use of a minimal set of local administrative accounts for certain maintenance and emergency activities. These special administrative accounts are not considered “user accounts” in the cases below.

- **Complete the NAF Deviation Request and Transition Plan.**

A template for the NAF Deviation Request and Transition Plan is available in Appendix B. Please refer to Appendix A as necessary to ensure the details required for the applicable use case have been included.

- **Route the NAF Deviation Request and Transition Plan through the center-defined routing path.**

  The Agency does not define internal routing methods for Centers. The Center is responsible for routing and concurrence from the Center NCAD POC and the Center CIO.

  If the deviation request impacts multiple centers, then concurrence of all Center NCAD POCs and Center CIOs is required.

- **Route the NAF Deviation Request and Transition Plan to the NCAD Project Manager.**

  The plan may be submitted through email as an attachment. In addition to encrypting the email if the plan contains sensitive information, each party should cryptographically sign the email and the email should be forwarded from party to party to maintain the path of approval in the body of the email (accepting the implied limitation of trust vouching through each party).

  The NCAD Project Manager will route the request through the appropriate OCIO channels, culminating in concurrence by the NASA CIO. All deviation requests are considered on a case-by-case basis.

  After the request is signed by the NASA CIO, or the CIO's representative, it will be forwarded to the NAF team for implementation, integration, and operation. No action will be taken by the NAF team until the signed form (or faxed copy) is received. After the approval is received by NAF, the NAF team will coordinate with the Author to plan for implementation.

  If Agency Sensitive Information (ASI: SBU, Classified, other) is included in the documentation the entire submittal must be encrypted.

- **Complete the NCAD-provided Interconnection Security Agreement (ISA).**

  All parties submitting a deviation request that will require a new trust to be established with the NAF forest (ndc.nasa.gov) must plan to complete an *Interconnection Security Agreement* as supplied by NCAD. This documentation does not have to be submitted with the deviation request. However, this documentation will need to be completed before a new trust is established.

  For a trust with a NASA internal system, the document *Internal Interconnection Security Agreement* will need to be completed.

  For systems external to NASA, there will be a larger set of documentation required. This documentation will be in accordance with NIST SP 800-47 and NIST SP 800-100. NCAD will supply further direction. Note: Interconnection with an external system *may* require recertification and reaccreditation of the systems involved (NAF and the external system).

  For help in determining whether a system is internal or external, consult NASA ITS-SOP-0033.

- **Respond to OCIO requests to review plan milestones and compliance throughout the Deviation Period.**

- **Notify the OCIO when the system is no longer in deviation and any trusts can be removed.**

Appendix A – Deviation Use Cases

The Deviation Request and Transition Plan covers the following two major types of cases:

- Center AD installations not capable of being migrated

  There are technical limitations which may prohibit migration, or prohibit efficient migration, of applications and services into the NAF forest. Resources that can not be migrated are captured in two of the use cases. Also, if a forest is scheduled to be decommissioned it may make migration prohibitively inefficient. Deviation Cases 1 and 2 address this situation.

- NAF AD trust with a third party

  Any trust with the NAF domain requires significant consideration in terms of operational, security, and architectural impact to NASA. The OCIO has determined the acceptable limits for authentication and authorization data flow. Existence of Agency AD installations when interoperating with NAF precipitate the need for trusts; therefore, the deviation cases encapsulate both AD installations and trusts.

Deviation Case 1 (DC#1)—CRF where the CRF contains resources only

Case Applicability

Existing Trust(s) with the Center Resource Forest (CRF) may not be able to be removed by the end of NAF migration or the CRF may house resources that cannot be migrated into the NAF. In these cases, a deviation request will be required to allow the Center Resource Forest (CRF) to continue to exist for a period of time after NAF migration.

The CRF will continue to contain resources that are accessed through the trust(s) or that cannot be migrated. The CRF will not contain user accounts.

Be aware that Mac users could be impacted. If the CRF continues to exist to house resources, then the Mac users which have migrated to the NAF will not be able to use NAF authentication to access these resource. Macs can not traverse forest trust boundaries.

Trust Details

In this deviation case, a trust with the NAF continues and only outbound trust(s) from the CRF to another domain or forest is allowed. The CRF trusts another domain or forest to be the identity source and supply the identity credentials. The CRF maintains a trust relation with the NAF to provide access for Agency users and/or continued administration.

The trust section of the plan must provide the following information:

- For the NAF trust, what are the explicit uses?
- For other non-NAF trust(s) (normally outgoing only—CRF must be the trusting forest, as user accounts will be emptied from the CRF as part of NAF migration)
  - Who the trust is with
  - What NASA applications/systems are accessed through the trust

Justification for the Deviation

The justification section of the plan must provide the following information as applicable:

- What resources remain? Reasons for inability to be migrated?

- What dependencies must be met to enable to resource to be migrated or decommissioned?
- Why can't the non-NAF trust(s) be removed after NAF migration?
- What are the dependencies that must be met to remove the trust?

Schedule for removal of the trust and CRF

The schedule section of the plan must provide the following information:

- Milestones for application/system migration or retirement
- Milestones for any dependencies

Plan for NAMS integration

The NAMS section of the application must provide the following information:

- Schedule for integrating the application/system into NAMS
- Plans for ensuring identities owning trusted accounts are captured in IdMAX
- In all cases, NAMS integration must take place prior to NAF migration

Deviation Case 2 (DC#2)—CRF where the CRF contains user accounts

Case Applicability

In this deviation case the CRF will continue to contain user accounts.

NOT PERMITTED

No deviations to allow the continued use of user accounts in the CRF will be permitted. All CRF user accounts must be moved to the NAF as part of NAF migration.

Deviation Case 3 (DC#3)—Legacy Resource Forest (LRF) where the LRF contains resources only

Case Applicability

In this deviation case an AD forest other than a CRF contains resources (applications/systems) that are problematic for migration into the NAF. Consideration will be given to specific problematic issues that prevent migration. However, in all cases the LRF will use the NAF identities for authentication—the LRFs will not host user accounts.

Trust Details

The LRF will operate through a trust with the NAF. If other trusts are employed then the following information must be supplied:

- Who the trust is with (MUST be outgoing—LRF must be the trusting forest)
- What NASA applications/systems are accessed through the trust

Justification for the Deviation

The justification section of the plan must provide the following information:

- Why can't the resources migrate to the NAF
- If applicable, why can't trusts (other than the NAF trust) be removed
- What are the dependencies that must be met to remove the trust and/or decommission the forest

Schedule for removal of the trust(s) and the LRF

The schedule section of the plan must provide the following information:

- Milestones for application/system migration or retirement
- Milestones for any dependencies

Plan for NAMS integration

The NAMS section of the application must provide the following information:

- Schedule for integrating the application/system into NAMS
- Plans for ensuring identities of trusted accounts are captured in NAMS
- In all cases, NAMS integration must take place prior to NAF migration

Deviation Case 4 (DC#4)—Trust with External Entities where the external entity uses NAF user accounts

Case Applicability

In this deviation case an AD forest that is external to NASA requires the use of NASA AD accounts for the purposes of authentication—the external organization trusts NASA accounts and authentications for the purposes of authentication and access control to external resources.

Trust Details

In the deviation case the external entity will require a one way trust with the NAF—the external entity will be the trusting domain.

- Does the external forest contain multiple domains? If so, does the trust have to include each of these domains?

Justification for the Deviation

The justification section of the plan must provide the following information:

- Explicit description of the external applications and services to be accessed
- Explanation of why NASA identities are required, e.g. explanation why NASA users can not use accounts supplied by the external entity
- Explicit description of impact if NAF accounts are not used—what is the impact to NASA/NASA users
- What are the dependencies that must be met to remove the trust and/or decommission the forest

Schedule for removal of the trust

The schedule section of the plan must provide the following information:

- Milestones for application/system migration or retirement
- Milestones for any dependencies

Trust creation prerequisites

In order for the trust to be created, the external organization must meet, or be prepared to meet, the following requirements:

- Accept and maintain a device certificate from the NAF system in order to support IPSec key exchange
- Accept endpoint transport mode IPSec ESP for all network traffic between NAF and the external organization's domain controller(s)
- Plan for utilizing the NAF identities to grant access control for resources (user accounts in the external organization will not have the authority to view the NAF directory)

Supplemental information

NASA requires an Interconnection Security Agreement in addition to the Devision Request and Transition Plan.

Emergency Disconnection

NASA reserves the right to unilaterally disconnect the trust. Reasons for emergency disconnection include detection of a system exploit or other contingency that jeopardizes NASA systems or data.

Deviation Case 5 (DC#5)—Retiring Resource Forest (RRF) where the RRF contains resources only

Case Applicability

In this deviation case an AD forest other than a CRF contains resources (applications/systems), but the forest is scheduled to be decommissioned. This forest will be called the Retiring Resource Forest (RRF). Migration of resources in the near term (within the NCAD schedule timeframe) is shown to be costly versus continued operation until the scheduled decommissioning. Case examples are forests to be decommissioned due to contract end of life.

Trust Details

The RRF will operate through a trust with the NAF. If other trusts are employed then the following information must be supplied:

- Who the trust is with (MUST be outgoing—RRF must be the trusting forest)
- What NASA applications/systems are accessed through the trust

Justification for the Deviation

The justification section of the plan must provide the following information:

- Why the resources cannot migrate to the NAF, or, cost justification for not migrating to NAF due to near term retirement date.

- If applicable, why trusts (other than the NAF trust) cannot be removed
- If applicable, description of the dependencies that must be met to remove the trust and/or decommission the forest

Schedule for removal of the trust(s) and the RRF

The schedule section of the plan must provide the following information:

- Milestones for application/system migration or retirement
- Milestones for RRF retirement
- Milestones for any dependencies

Plan for NAMS integration

The NAMS section of the application must provide the following information:

- Whether the application/system will into NAMS prior to retirement
- Plans for ensuring lifecycle management of accounts if NAMS is not used

Deviation Case 6 (DC#6)—Retiring Forest (RF) where the RF contains user accounts

Case Applicability

In this deviation case the RF contains user accounts in addition to resources. Migration of resources and user accounts in the near term (within the NCAD schedule timeframe) is shown to be costly versus continued operation until the scheduled decommissioning. Case examples are forests to be decommissioned due to contract end of life.

Trust Details

If NASA worker access is required for resources in the RF then the RF will operate through a one-way trust with the NAF. The RF will trust the NAF and NAF user accounts for purposes of granting access. The NAF will not trust the RF (the NAF will not trust the identities and user accounts in the RF). If other trusts are employed then the following information must be supplied:

- Who the trust is with
- What NASA applications/systems are accessed through the trust

Justification for the Deviation

The justification section of the plan must provide the following information:

- Why the resources cannot migrate to the NAF, or, cost justification for not migrating to NAF due to near term retirement date
- Why the user accounts cannot migrate to the NAF
- If applicable, why trusts (other than the NAF trust) cannot be removed
- If applicable, description of the dependencies that must be met to remove the trust and/or decommission the forest

Schedule for removal of the trust(s) and the RF

The schedule section of the plan must provide the following information:

- Milestones for application/system migration or retirement
- Milestones for RF retirement
- Milestones for any dependencies

Plan for NAMS integration

The NAMS section of the application must provide the following information:

- Whether the application/system will integrate into NAMS prior to retirement
- Plans for ensuring lifecycle management of accounts if NAMS is not used
- Plans for ensuring identities owning accounts in the RF are captured in IdMAX

Appendix B – NAF Deviation and Transition Form

The NAF Deviation Request and Transition Plan codifies a deviation process that culminates with the NASA CIO approval. It provides a mechanism for continued operation of Active Directory in deviation with the Agency requirement for a single domain architecture.

Requestor:	
Phone:	
E-mail:	
Requesting Organization:	
Date:	

Forest Name:	

Overview of forest/domain architecture (additional documents may be attached at the submitter's preference)

Forest/domain Architecture:

For NASA forests, the forest security plan certification and accreditation information of the new trusted domain must be entered below. Additional documents may be attached at the submitter's preference.

Security Plan Information (ATO Number):

Author:	
Phone:	
E-mail:	

Reviewed:	
NCAD Center POC:	
Date:	

Concurrence:	
Center CIO:	
Date:	

Concurrence:	
NCAD Program Manager:	
Date:	

Approval:	
Agency CIO or Designee:	
Date:	

NAF *Deviation* and Deviation Transition Plan—Plan Details

Case Applicability

Define the type of deviation being requested, referencing one of the predefined use case types from section 6. Explain how and why this case relates to the use case type selected.

Trust Details

Provide trust information and description as required per use case type.

Justification for the Deviation

Provide justification information as recommended per use case type.

Schedule for removal of the trust and/or forest

Provide milestones as recommended per use case type.

Plan for NAMS integration

Provide NAMS integration information as recommended per use case type.

Glossary

Acronym	Term	Explanation
AD	Active Directory	Microsoft Windows Active Directory
CIO	Chief Information Officer	
CRF	Center Resource Forest	
IdMAX	Identity Management and Account eXchange	The Agency system that provides Identity and Access Management Tools
LRF	Legacy Resource Forest	An AD forest at NASA that is not a Center Resource Forest (CRF)
MSFC	Marshall Space Flight Center	
NAF	NASA Agency Forest	The Agency Forest that supports AD authentication
	NAF Domain	The name of the NAF Domain is ndc.nasa.gov
NAMS	NASA Account Management System	The Agency Account Management System is part of IdMAX, and governs account management to the NAF.
NCAD	The NASA Consolidation of Active Directory	Project that is responsible for the establishment of the NASA Agency Forest (NAF), and migration from Center AD Domains to the NAF
NDC	NASA Data Center	The NASA Data Center manages the NAF.
OCIO	Office of the Chief Information Officer	
RF	Retiring Forest	A forest that contains both users and resources, and will be retired according to an approved deviation schedule.
RRF	Retiring Resource Forest	A forest that contains resources, but no users, and will be retired according to an approved deviation schedule.
	Trust	The AD trust relationship is a logical mechanism by which users can be authenticated in one domain and be granted access to resources in another domain.

Approval

8-5-08

Willard F. Peters
NASA Enterprise Architect

Date