Standard Operating Procedure

Procedures for Submitting an Application Integration Deviation Request and Transition Plan

EA-SOP-0004

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 an Application Integration 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 Application Integration Compliance Schedule. Details of the Compliance Requirements and Schedule are found in EA-STD-0001, *Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorization Infrastructure*.

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

- Deviations from NASA Account Management System (NAMS) Integration
- Deviations from integration into the NASA Authentication and Authorization Architecture

The Deviation Request and Transition Plan differs from a waiver in that while the deviation process recognizes that certain Centers and/or Mission Directorates can not fully comply with Application Integration requirements, it does not provide a variance to the requirement to integrate into the NASA Infrastructure. Instead this deviation process allows for deviations under specific circumstances and mandates a corresponding Deviation Transition plan that defines when the Center/Mission Directorate will be able to integrate into the NASA Infrastructure or decommission the Application.

Scope

This SOP applies to all NASA applications as defined in EA-STD-0001.

Applicable Documents

- EA-STD-0001, August 2008, “Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorization Infrastructure”
- 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 800-63, April 2006, “Electronic Authentication Guideline” http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- NIST Special Publication 800-82, September 28, 2007, “DRAFT Guide to Industrial Control Systems (ICS) Security” http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.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 Account Authorization Official (AAO)**

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

- **Center CIO**

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

- **Logical Access Control Integration Lead**

  Review and provide concurrence/non-concurrence with the submitted request. Route through NASA OCIO.

- **NASA CIO**

  Provide final concurrence/non-concurrence with the submitted request, and inform the Logical Access Control Integration Lead of the decision.

Process

The organization within the requesting Center will utilize the following procedures to create an Application Integration Deviation Request and Transition Plan:

- **Identify the applicable deviation case**.

  The following cases have been identified and may be considered for eligibility to deviate from the Application Integration Compliance Requirements.

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

Table 1 -- Deviation Case Summary

Case	Name (Deviation Case Type)
1	Application will be retired by September 30, 2011 and will not integrate into NAMS
2	Application will be retired by September 30, 2012 and will not integrate with the NAF or eAuthentication
3	Application cannot be integrated into NAMS by the compliance deadline
4	Application cannot use the NAMS Generic workflow
5	Application cannot integrate with either the NAF or eAuthentication by the compliance deadline
6	Application cannot integrate with either the NAF or eAuthentication due to technology constraints

.

- **Complete the Application Integration Deviation Request and Transition Plan.**

  A template for the 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 Application Integration 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 AAO and the Center CIO.

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

- **Route the Application Integration Deviation Request and Transition Plan to the Logical Access Control Integration Lead.**

  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 Logical Access Control Integration Lead 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 requesting organization for implementation.

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

- **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.**

Appendix A – Deviation Use Cases

Deviation Case 1 (DC#1)— Application will be retired by September 30, 2011 and will not integrate into NAMS

Case Applicability

Applications that will be retired by September 30, 2011 may be allowed to maintain current account management processes until the application is retired. In general, this deviation case is applicable only to those applications that will be retired within one year of the published compliance date in EA-STD-0001. (The compliance dates are based on FIPS 199 Risk categories and information sensitivity.) The Application Owner will have to ensure that the spirit of NAMS is met.

Application Details

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

- Application Name
- NAMS Number - Refer to the NASA Application Tracking Tool (NATT)
- Responsible NASA Official
- Description

  FIPS 199 Risk Category
- Expected Retirement Date

Justification for the Deviation

The justification section of the plan must address the following questions:

- What application(s) interface with the existing application?
- What are the dependencies that must be met in order to retire the application?
- What application(s) will replace the functionality provided by the existing application?

Schedule for retirement of the application

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

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

Plan for meeting the spirit of NAMS integration

The NAMS section must provide the following information:

- Plans for ensuring lifecycle management of accounts if NAMS is not used
- Plans for ensuring identities owning accounts in the application are captured in IdMAX

Deviation Case 2 (DC#2)— Application will be retired by September 30, 2012 and will not integrate with the NAF or eAuthentication

Case Applicability

Applications that will be retired by September 30, 2012 may be allowed to maintain current authentication processes until the application is retired. In general, this deviation case is applicable only to those applications that will be retired within one year of the published application integration compliance date in EA-STD-0001. (The compliance dates are based on FIPS 199 Risk categories and information sensitivity.) The Application Owner will have to ensure that the spirit of central authentication is met.

Application Details

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

- Application Name
- NAMS Number (Refer to NATT)
- Responsible NASA Official
- Description
- FIPS 199 Risk Category
- Expected Retirement Date
- Current authentication source
- Current authentication credentials

Justification for the Deviation

The justification section of the plan must address the following questions:

- What application(s) interface with the existing application?
- What are the dependencies that must be met in order to retire the application?
- What application(s) will replace the functionality provided by the existing application?

Schedule for retirement of the application

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

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

Plan for meeting the spirit of central authentication integration

The Central Authentication section must provide the following information:

- Plans for ensuring identities owning accounts in the application are captured in IdMAX
- Plans for ensuring lifecycle management of authentication credentials tied to identities in IdMAX
- Plans for ensuring authentication credentials meet proper level of assurance for the FIPS risk category of the application

Deviation Case 3 (DC#3)— Application cannot be integrated into NAMS by the compliance deadline

Case Applicability

In this deviation case the application will be integrated into NAMS, but cannot be integrated by the compliance deadline.

NOT PERMITTED

This deviation is not allowed. Any application that cannot meet the NAMS integration compliance deadline, and is not scheduled to be retired within one year of the compliance deadline (DC#1), will be carried as a non-compliance on Agency reports and Center stoplight charts until the application is integrated into NAMS.

Deviation Case 4 (DC#4)— Application cannot utilize the NAMS Generic workflow

Case Applicability

In this deviation case the application can integrate with NAMS, but cannot use the NAMS Generic workflow. A custom workflow is planned for NAMS integration.

Application Details

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

- Application Name
- NAMS Number (Refer to NATT)
- Responsible NASA Official
- Description
- FIPS 199 Risk Category
- Expected Retirement Date

Justification for the Deviation

The justification section of the plan must address the following questions:

- Why can't the NAMS Generic workflow be used?
- What features must be added to the NAMS Generic workflow in order for it to meet the requirements of the application?
- What types of manual workarounds were considered, and why can't they be utilized with the NAMS Generic workflow to meet the requirements of the application?
- What Service Requests (SRs) have been submitted to request changes to the NAMS Generic workflow to meet the requirements of the application?

Schedule for integration of the application

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

- NAMS integration schedule
- Milestones for application/system migration to NAMS Generic workflow, or retirement
- Milestones for any dependencies

Plan for maintaining the NAMS Custom workflow

The maintenance section must provide the following information:

- Plans for ensuring lifecycle management of the NAMS custom workflow, including modification and testing of the workflow when the NAMS framework is updated.

Deviation Case 5 (DC#5)— Application cannot integrate with either the NAF or eAuthentication by the compliance deadline

Case Applicability

In this deviation case the application can integrate with either the NAF or eAuthentication; however, integration cannot be completed by the compliance deadline in EA-STD-0001.

Application Details

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

- Application Name
- NAMS Number (Refer to NATT)
- Responsible NASA Official
- Description
- FIPS 199 Risk Category
- Expected Retirement Date
- Current authentication source
- Current authentication credentials

Justification for the Deviation

The justification section of the plan must address the following questions:

- Why can’t the compliance date be met?
- What are the dependencies that must be met in order to integrate the application?

Schedule for integration of the application

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

- NAMS integration schedule
- Milestones for application/system migration or retirement
- Milestones for any dependencies

Plan for meeting the spirit of central authentication integration

The central authentication section must provide the following information:

- Plans for ensuring identities owning accounts in the application are captured in IdMAX
- Plans for ensuring lifecycle management of authentication credentials tied to identities in IdMAX
- Plans for ensuring authentication credentials meet proper level of assurance for the FIPS risk category of the application

Deviation Case 6 (DC#6)— Application cannot integrate with either the NAF or eAuthentication due to technology constraints

Case Applicability

In this deviation case the application cannot integrate with either the NAF or eAuthentication due to technology constraints.

Application Details

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

- Application Name
- NAMS Number (Refer to NATT)
- Responsible NASA Official
- Description
- FIPS 199 Risk Category
- Expected Retirement Date
- Current authentication source
- Current authentication credentials
- Commercial Off-the-Shelft (COTS) product(s) being used (if any)

Justification for the Deviation

The justification section of the plan must address the following questions:

- Why can't the application be integrated with either the NAF or eAuthentication?
- What are the dependencies that must be met in order to integrate the application?
- What are the long-term plans for removing technology constraints?
- What analysis was performed to determine the best alternate method?
- If the application will use RSA SecureID tokens, will the application be migrated to the Agency RSA infrastructure when available, or does it require a separate RSA instance? If the latter, why can't the Agency RSA infrastructure be used?

Schedule for integration of the application

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

- NAMS integration schedule
- Milestones for application/system migration or retirement
- Milestones for any dependencies

Plan for meeting the spirit of central authentication integration

The cemtral authentication section must provide the following information:

- Plans for ensuring identities owning accounts in the application are captured in IdMAX
- Plans for ensuring lifecycle management of authentication credentials tied to identities in IdMAX
- Plans for ensuring authentication credentials meet proper level of assurance for the FIPS risk category of the application

Appendix B – Application Integration Deviation Request and Transition Form

The Applicaition Integration Deviation Request and Transition Plan codifies a deviation process that culminates with the NASA CIO approval. It provides a mechanism for continued operation of an application in deviation with the Agency requirement for a central identity and access management architecture.

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

Application Owner:	
Phone:	
E-mail:	

Concurrence:	
Center AAO:	
Date:	

Concurrence:	
Center CIO:	
Date:	

Concurrence:	
Logical Access Control Integration Lead:	
Date:	

Approval:	
Agency CIO or Designee:	
Date:	

Application Integration Deviation Requestion and Transition Plan

1. *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.

2. *Application Details*

Provide application details as required per use case type.

3. *Justification for the Deviation*

Provide justification information as recommended per use case type.

4. *Schedule*

Provide the appropriate schedule and milestones as recommended per use case type.

5. *Plan for meeting the spirit of NAMS and/or central authentication integration*

Provide information as recommended per use case type.

Glossary

Acronym	Term	Explanation
AAO	Account Authorization Official	The Account Authorization Official is responsible for application integration into NAMS and the authentication architecture.
CIO	Chief Information Officer	
COTS	Commercial Off-the-Shelf	Refers to software that is commercially available, rather than being developed in-house.
	eAuthentication	eAuthentication provides central authentication and authorization for web-based applications.
FIPS	Federal Information Processing Standard	
HSPD-12	Homeland Security Presidential Directive 12	
IdMAX	Identity Management and Account eXchange	The Agency system that provides Identity and Access Management Tools
ITS-SOP	Information Technology Security Standard Operating Procedure	
NAF	NASA Agency Forest	The Agency Forest that supports AD authentication
NAMS	NASA Account Management System	The Agency Account Management System is part of IdMAX, and governs account management to the NAF.
NATT	NASA Application Tracking Tool	The NASA Application Tracking Tool is NASA's application registry. NATT also provides support for NAMS integration. NATT is found at: https://www7.jsc.nasa.gov/natt/
NIST	National Institute for Standards and Technology	
NPR	NASA Procedures and Requirements	
OCIO	Office of the Chief Information Officer	
RSA		RSA securID tokens provide two-factor authentication. (Note: RSA is not an acronym.)

SBU	Sensitive But Unclassified	

Approval

8-5-08

Willard F. Peters
NASA Enterprise Architect

Date