NASA Integrated Services Environment

Sharon Ing
NISE Project Manager
sharon.ing@nasa.gov
October 2005
Agenda

- What is NISE?
- Today’s Environment
- To Be Environment
- Architecture
- Data Flow
- Process
  - Strategy
  - Organization
  - Three-legged stool
  - Security
- Status
- Summary
- Questions?
NISE – Project Scope

NISE Consists Of Four Major Areas Of Focus:

- **Identity Management System (IDMS)**
  - IDMS will be the authoritative single source of validated identities for NASA. IDMS will provide a central repository of identity information.

- **Cyber Identity Management System (CIMS)**
  - CIMS will provide a unified Enterprise Directory for retrieving end user identity information.
  - CIMS will ensure the transparent and secure exchange of identity across the Agency.

- **NASA Account Management System (NAMS)**
  - NAMS will provide consistent and accurate account management across the Agency. NAMS will allow immediate changes to user accounts throughout the system. NAMS Center managers – known as Account Authorization Officials (AAO) – are involved in architecting, testing, and vetting a uniform set of Agency processes needed to establish consistent account management business processes and support for use in all NASA locations.

- **NASA E-Authentication Initiative**
  - This initiative will allow identity credentials to be passed between most applications without additional authentication using the Inside NASA Web Portal service as its foundation. The NISE E-Authentication service will help to improve productivity and user satisfaction by providing Web Single Sign On (SSO) for Agency applications.

Depends on Common Badging Access and Control System (CBACS)
NISE in the Context of NASA IT

Integrated Information Infrastructure Program (IIIP)

Communications Services

Security Services

Computing Services

NISE

CBACS

NAMS

Central Account Information Repository

NAMS

Central Directory Services

NAMS

Central IDMS

Central Identity Information Repository

“Proofed Identity”
NISE – Services Model

NISE is a central integrated IT infrastructure that interacts with other account management systems.

E-Authentication Portal

SSO Across Agency Applications

to Federal E-Authentication Gateway

CBACS Project

NDC Active Directory Services
• **Identity Management System**
  – No single reliable Agency source of personal identity to support account provisioning requirements.
  – Identity management processes are largely manual, labor intensive and disjointed – duplicative identity information and administration.

• **Cyber Identity Management System**
  – 10 years old – Agencywide X.500 directory service is not able to support identity management needs / directory enabled applications.
  – These are independently managed directories – pieced together to form Agency directory – struggling to provide enterprise-level service.

• **NASA Account Management System**
  – Many Agency applications do not have a comprehensive methodology for tracking which individuals have access to what information and resources.
  – Agency applications do not have the means to effectively coordinate management of their accounts between different Agency applications.

• **NASA E-Authentication Service**
  – Many applications have their own source for authentication, causing users to have multiple userid’s and passwords.
  – From user’s view, E-Authentication services will provide web Single Sign On (SSO) by allowing identity credentials to be passed between applications without additional authentication.
NASA Agencywide “As-Is” Overview Summary

12 major sites = at least 12 ways each to perform –

- Account Management / Provide Directory Services / Manage Identities

Thumbnail Analysis: 3 “general techniques” / Center X 3,000
NASA IT applications = 9,000 tailored application processes
NISE “As-Is” Architecture

TODAY – Multiple User Names and Passwords
“To-Be” NISE Components
A Layered View

• User:
  – Simple sign-on to systems integrated into the foundation using passwords
  – Quick set-up to multiple accounts
  – Common badge that works at all Centers
  – Automated password reset
  – One stop shopping for directory information

• NASA Management and Application Owners
  – Single reporting/management capability
  – Reduced password maintenance
  – Quick account set-up and deletion of accounts
  – Strong audit capability and consistent account processes across the Agency
  – Single source for identity information for all people working for/with NASA
  – Moves from multiple ways to do the same thing, to one system
  – Corrects long-standing security and internal controls weakness
NISE “To-Be” Architecture

NISE SSO Has Critical Dependency on Inside NASA Web Portal
“To-Be” NISE Components
HSPD-12 Compliance

- **User:**
  - (Same as NISE, plus)
  - Single sign-on to all systems using SmartCards and PKI
  - Quick set-up and access to all accounts
  - Physical access to authorized facilities

- **NASA Management and Application Owners**
  - (Same as NISE, plus)
  - Increased assurance that system users are authorized the appropriate degree of access
  - Decreased password resets and trouble calls
  - Central reporting/management capability
  - Physical access control
  - Compliance with HSPD-12
NISE Target Application Architecture

Key
- Provisioned Sources
- Synchronization Sources
- NISE Infrastructure

Provisioned Sources:
- IRIS
- FNMS
- NCTS
- UUPIC
- FPPS

Synchronization Sources:
- IDMS

NISE Infrastructure:
- ARC
- DFRC
- GRC
- GSFC
- HQ
- IVV
- JPL
- JSC
- KSC
- LaRC
- MAF
- MSFC
- SSC
- WFF
- WSTF

Self Validation:
- CBACS

Identity Validation:
- Sun IdM

Federal Bridge
- c=US

PKI X.500

OneNASA EMail

Public LDAP
- nasa.gov

Enterprise LDAP
- nasa.gov

Provisioned Sources:
- NISE
- Infrastructure

NISE Target Application Architecture
NISE Identity Requirements

✔ Provide Consistent Processes to Manage Identity Information

• Establish Identities in IdM Prior to Granting Access to Systems
  • NISE Identity Repository
  • Unique Personal Identifier Is Required for Identity Management
  • Identities Must Get a UUPIC Before Adding To Identity Manager Server
• All Identities Are Labeled With Validation Status “Code”
  • 0 = Non-verified – Identity Data Provided By a Non-trusted Source
  • 1 = Verified – Identity Cross-referenced With Trusted or Validated Data Source or Verified by a COTR
  • 2 = Validated – Identity and Credentials Validated by a Security Official.
• CBACS processes will provide physical validation of the Authoritative Identity Repository
Payroll Data Process

- Today NASA Civil Servant Payroll Data Is Processed in Support of the IFM Travel Manager Application
- Active Nasa Civil Servants Input to X500 System Via Payroll File
- Data Provided – SSN, Center Code, Surname, First Name, MI, Suffix, Separation Date and UUPIC
One NASA Email Data

- User Records From One NASA Email Database Provided to Identity Interface Server – Which Assigns UUPIC Numbers for –
  - **Civil Servant Records** – Attempt Match to Existing Identities
  - **Contractor Records** – Assigned UUPIC Based on Name, Email, Center Code & Unique ID
- UUPIC Provided to Center Via Existing One NASA File Exchange
- Email Data Is Passed to Identity Manager Via IdM DB Store
Center Employee Data

- Center Data Warehouses / Badging Systems Have Valuable Identity Information However –
  - This Information Is Sometimes Out of Date and Inaccurate
  - May Contain Personnel Not Linked to NASA Business Needs
- For NISE – Center Identity Information Will Be “One-Time” Load
  - Goal – Capture Information Not Found in Payroll or One NASA Email
- Future – Center Identity Information Will Be Maintained in CBACS Regional Databases & Passed to IdM Via CBACS Central Region
Enterprise LDAP Provisioning

- LDAP Directory Will Use Standard InetOrgPerson and Extended NASAPerson Objectclass
- All Civil Servants, Contractors, and Virtual Identities Will Be Maintained in Directory – Visitors Will Not Be Provisioned to the Directory
Account Management

- Four Steps in IT accounts life cycle
  - Request an account
  - Create an account
  - Maintain an account
  - Close an account
- Many sub-steps support these high-level steps
- Special cases / situations may require changes in the details or flow of these steps
- For example, the steps used to create an IT account for a civil servant in the NASA time card system are very different from the steps to create an IT account for a scientist in another country – collaborating on an experiment
Create and Modify Account Request on the Framework

- Request User Interface

1. Supervisor/Sponsor identified?
   - Yes: Identify Supervisor/Sponsor
   - No: Creating new Identity?
     - Yes: Create New Identity
     - No: Provide Interface to Find Identity

2. Identities Found > 1
   - Yes: Provide Interface to List Identities
   - No: Identity Chosen

3. Present Identity details to verify correct user
   - Correct User?
     - Yes: Select Applications/Resources
     - No: Create New Identity

4. Enter Required and Optional Attributes and Validate

Any time a form is presented to the user prior to submitting the task a 'cancel' option is available to abort the process.

Applications will be stored as application groups in IdM. We will use a naming convention to keep them categorized. For now we will divide them up into Agency Wide and Center wide applications.

Custom forms 1 per application. The form is only presented if the application is requested. The forms provide validation of data entered.
Create and Modify Account Request on the Framework (cont)

---

**Workflow Submitted**

- **New Identity Request?**
  - Yes
    - **New Identity Account(s) request**
      - This callout encapsulates the 1.1 Prepare NASA Initial New user flows.

- **Global Approval Workflow**
  - This encapsulates the 1.1 and 1.2 portions that require the Associate AAO's eyes.

---

**Asynchronous Parallel Execution**

- **Process App1 Approval Workflow**
  - **Process App1 Provisioning Workflow**

- **Process App2 Approval Workflow**
  - **Process App2 Provisioning Workflow**

- **Process AppN Approval Workflow**
  - **Process AppN Provisioning Workflow**

---

Custom flows for applications. These will be developed for the complex approval/provisioning processes. We will otherwise provide generic processes. This encapsulates the 2.0 Create User flows.
NISE Requirements Validation Strategy

- **Dec 2003**: Formulated NISE integrated services infrastructure approach for Agency applications. CIMS & NAMS Teams have Center members.
- **March 2004**: Contracted with expert vendors to perform market analysis and planning related to product and technology alternatives.
- **June – July 2004**: 
  - Reviewed alignment with IIIP, NASA & Federal guidance (e.g., NIST).
  - Evaluated approach, implementation, providers, and pricing alternatives.
  - Interviewed government and commercial references.
- **July 2004**: Product decision review for NASA CIO Office & approved to procure Sun Java Identity Manager and directory solution.
- **September 2004**: Stood up hardware & software at MSFC and trained staff.
- **Nov 2004**: Conducted Preliminary Design Review (PDR).
- **Feb 2005**: Conducted Preliminary Technical Readiness Review (TRR).
- **May 2005**: Conducted Project Technical Assessment External Review.
- **August 2005**: Conducted NISE Enterprise Architecture Review.
- **October 2005**: Plan – Conduct IOC Operational Readiness Review (ORR).
NISE Executive Sponsorship / Project Organizational Structure

IIIP Program Manager
NASA CIO

Deputy CIO for IT Security
NISE Program Executive

Chief Technology Officer

NASA CIO Council
NASA CIOs

Program Management Council
Marshall Space Flight Center CIO

MSFC Office of the CIO
Agencywide IT Services Manager

NISE Project Manager

Identity Management System (IDMS)
Team Lead (MSFC)

Cyber Identity Management System (CIMS)
Team Lead (LaRC)

NASA Account Management System (NAMS)
Team Lead (GSFC)

E-Authentication Initiative
Team Lead (ARC)
NAMS Base Philosophy: Enterprise IT

• Enterprise IT is a “three-legged stool”
  – **IT Management Architecture**: Policy, Metric Parameters, Governance, Reporting Requirements, Architectural Life Cycle Management, Security Mandates, Staffing
  – **IT Business Architecture**: Processes, Procedures, Funding, Operational Life-Cycle Management, Customers, Metrics Tracking, Reporting Methodologies, Security Assurance, Training, Certification
  – **IT Technical Architecture**: Systems, COTS, Applications, Automation, Integration, Security Techniques

All too often, Enterprise IT is missing out on the management leg of the stool...

>>And all three “legs” MUST be complete, robust, integrated, supporting, and complementary for success!
### NISE Components Phasing

**NIST Life Cycle Phase Progress – CDR**

<table>
<thead>
<tr>
<th>NISE Component</th>
<th>Phase 1 Initiate</th>
<th>Phase 2 Dev/Buy</th>
<th>Phase 3 Implement</th>
<th>Phase 4 O&amp;M</th>
<th>Phase 5 Dispose</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDMS</td>
<td>COMPLETE</td>
<td>COMPLETE</td>
<td>IN WORK</td>
<td>PLANNED</td>
<td></td>
</tr>
<tr>
<td>CIMS</td>
<td>COMPLETE</td>
<td>COMPLETE</td>
<td>IN WORK</td>
<td>PLANNED</td>
<td></td>
</tr>
<tr>
<td>NAMS</td>
<td>COMPLETE</td>
<td>COMPLETE</td>
<td>IN WORK</td>
<td>PLANNED</td>
<td></td>
</tr>
<tr>
<td>E-AUTHENTICATION</td>
<td>COMPLETE</td>
<td>COMPLETE</td>
<td>IN WORK</td>
<td>PLANNED</td>
<td></td>
</tr>
</tbody>
</table>

- E-Authentication Phasing has made quick progress because of potential benefits for Agencywide SSO
NISE Security Plan

• NIST SP 800-18 – Security Plans
  – NISE Sun IdM IT Security Plan
  – NISE Sun IdM IT Security Plan
  – NDC IT Directory Security Plan
  – Final Security Plan Will Be Complete by NISE ORR

• NIST SP 800-60 – Information Systems / Security Categories
  – Impact levels for management & support information assigned
certifications documented in Security Plan

• Security technical requirements for interfaces and
communications protocols listed in detailed design section

• NISE component configuration comply with NIST Security
Guidelines, NPR 2810, and Section 508 requirements
NISE System Life Cycle
NIST SP 800-18 Phasing Model View

Requirements Review 4/27
Approval to Procure 7/20
PDR 11/4
CDR 1/6
PTA 5/24
IATO 2/28
7120 Review 7/21
ORR IOC 10/25
Agency Services ORRs

Phase I
Agency Services
Implementation

Phase II
Center Services
Implementation

Testing

10/1/2003
Market Analysis & Blue Print Design

10/1/2004
Begin Phase I Ops

10/1/2005
Begin Phase II Ops

10/1/2006
Fully Implemented

10/1/2007
Operations & Maintenance

Initiation
Acquisition & Development

Initiation
Acquisition & Development

CBACS Integration & E-Authentication

Ear Review 8/29

Center-Level ORRs
Summary

• Strong “teamworking” approach required to win
• Solid Communications plan – stay on message
• Requires investing in implementation team skills
• Plan, build, and test – plan, build, and test – and repeat as required...to get it right.

Our overall IT Security posture is enhanced by integrating and centralizing application authentication, account management, and identity management infrastructures using consistent, verified, and validated processes.
Questions??
Abstract:

This presentation will begin with a discussion on NASA’s current distributed environment for directories, identity management and account management. We will follow with information concerning the drivers, design, reviews and implementation of the NISE Project. The final component of the presentation discusses processes used, status and conclusions.