Common Badging and Access Control System (CBACS)

Marshall Space Flight Center

October 4, 2005
portia.dischinger@nasa.gov
Agenda

- Beginning: Smart Cards
- Re-direction: CBACS
- CBACS Description
- CBACS Integration
- CBACS Deployment
- Milestones and Dependencies
- Risks
- Planning
- Next Steps
- Summary
CBACS History

- Started in 2003 as NASA Smart Card Project
  - Implementation of a multi-application, multi-technology Smart Card program for the Agency
  - Issued GSA task order in November 2003
  - Conducted NASA site surveys in February - March of 2004
- During site surveys, determined that Center badging infrastructures were non-standard/non-compatible with Smart Card technology
- Re-directed the program to incorporate a common badging and access control solution for the Agency, known as CBACS
  - Smart Cards for logical and physical access will be implemented in the final phase
CBACS – Initial Scope – Smart Cards

- **MISSION:** (2002/2003)
  - The Implementation of a multi-application, multi-technology smart card program with an Agency user base

- **GOALS:**
  - To issue a common credential token (*physical and logical identifier*) that is….
    - Used by NASA employees, contractors, and other people approved by NASA….
    - Who require routine access to NASA physical and information resources.
    - An inter-agency Federal Identity Credential conforming with emerging federal policy and technical interoperability

*During Site Surveys, issues were determined on several fronts: diversity of existing PACS, need for common processes, difficulties in logical roll-out, and flexibility/ease of use of system*
IDMS – Identity Management System
CCMS – Central Card Management System

LDAP – Lightweight Directory Access Protocol
CA = Certificate Authority
SSLv3
PI = Person Identifier (Contained in FIC-N)
PI = Uniform Universal Person Identifier (UUPIC)

PACS – Physical Access Control System

Employee Data, FIC-N
Name, SSN, DOB
Name, FIC-N, Legacy Prox
PI, Legacy Prox
PI

CCMS
IDMS Integration
LDAP
Card ID DB

Employee Data, FIC-N
Registration Data & Legacy Prox

LDAP
SSLv3
Encryption
Certs & CRLs

Agency Directory
LDAP
Encrypt
Certs &
CRLs

Certificate Verification

Logical Access (ActivClient)

Enrollment
Digital Camera
Fargo Printer (w/ magstripe)
Smart Card
Contactless
Legacy Prox

Existing Identity DB

Security
HR

PACS
ACL

Smart Card
Legacy Prox

CBACS – Project Re-Direction

  - Achieve high business value through a common badging and access control system that integrates with Smart Cards

- GOALS:
  - Initially provide physical (versus logical) deployment of through CBACS
    - Provides a common consistent and reliable environment into which to release the Smart Card
    - Gives opportunity to develop Agency consistent processes, practices and policies
    - Enables Enterprise data capture and management
    - Promotes data validation prior to SC issuance
    - Avoids further investment in current PACS systems
CBACS - Description

An **Integrated** Services and IT Security Environment That Fulfills NASA and Homeland Security Presidential Directive (HSPD-12) Requirements for:

- **NASA Identity Management System** – **IDMS**
  - Central Authoritative Source for Personnel Identification
  - Warehouse for Personnel Security Investigation Determinations
  - Warehouse for Clearance Issuance & Uniform Universal Person Identification Code (UUPIC)

- **Enterprise Physical Access Control System** – **E-PACS**
  - Software for Common Badging Application
  - Area Access Management
  - Visitor Management System (Optional)
  - Alarm Monitoring Application
  - Integrated Digital Video Recording and Archiving System

- **Smart Card Physical Access** – **SC**
  - Hybrid Smart Card
  - Utilized with E-PACS for Physical Access
  - Provide Logical Access to NASA Computerized Systems During Final Phase of Implementation

- **Central Card Management System** – **CCMS**
  - Contact and Contact-less Smart Card Encoding
  - Provides Logical Certificates to the Smart Card from the NASA CA
  - Smart Card Life Cycle Management
## CBACS - System Life Cycle

<table>
<thead>
<tr>
<th></th>
<th>IDMS</th>
<th>E-PACS</th>
<th>Smart Card</th>
<th>CCMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiation</strong></td>
<td>Complete</td>
<td>Complete</td>
<td>Complete</td>
<td>Complete</td>
</tr>
<tr>
<td><strong>Development and Acquisition</strong></td>
<td>Complete</td>
<td>Ongoing</td>
<td>Ongoing</td>
<td>Ongoing</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td>Ongoing</td>
<td>Ongoing</td>
<td>Lab</td>
<td>Lab</td>
</tr>
<tr>
<td><strong>Operations and Maintenance</strong></td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>Disposal</strong></td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

**NIST Phasing Model View**
Target Architecture

Key
- Provisioned Sources
- Synchronization Sources
- NISE Infrastructure

IDMS

PKI X.500

Federal Bridge

OneNASA EMail

sun.idm

ARC
DFRC
GRC
GSFC
HQ
IVV
JPL
JSC
KSC
LaRC
MAF
MSFC
SSC
WFF
WSTF

ARC AD
DFRC AD
GRC AD
GSFC AD
HQ AD
IVV AD
JPL AD
JSC AD
KSC AD
LaRC AD
MAF AD
MSFC AD
SSC AD
WFF AD
WSTF AD

Public LDAP

Enterprise LDAP

nasa.gov

nasa.gov

nasa.gov

Identity Validation

Self Validation

Enterprise AD

Contacts and Users

Synchronization Sources

Provisioned Sources

NISE Infrastructure

PKI

NISE Infrastructure

Identity Validation

OneNASA EMail

Enterprise AD

Contacts and Users

Identity Validation

Self Validation

Enterprise AD

Contacts and Users
CBACS Enrollment Process

- **Requirement**
  - HSPD-12 (3) “Secure and reliable forms of identification” that (a) is issued based on sound criteria for verifying an individual employee’s identity; … issued only by providers whose reliability has been established by an official accreditation process

- **Enrollment Process Definition**
  - The process of issuing a card to a cardholder within the One NASA system is defined in four phases:
    - Registration
    - Verification
    - Validation
    - Issuance
CBACS Deployment

Agency Active Directory

IDMS

Master Server

Central Regional Server

NISE

UUPIC

Centers with Regional Database

Regional Server

Enrollment station

Centers without Regional Database

Enrollment station

Enrollment station
## CBACS Major Milestones and Dependencies

<table>
<thead>
<tr>
<th>Major Milestones</th>
<th>Date</th>
<th>CBACS Project Dependencies</th>
<th>Other Project Dependencies</th>
<th>Proposed Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue One NASA Badge To Civil Servants</td>
<td>July 2005</td>
<td>Badge Issuance Workstations&lt;br&gt;Central Region And Master Server</td>
<td>NISN - WAN Connectivity To Central Region Server&lt;br&gt;NDC/Center Trust Relationship Highly Desirable</td>
<td>Complete</td>
</tr>
<tr>
<td>Issue One NASA Badge To All Employees Without WAN</td>
<td>Jan 2006</td>
<td>Deploy Regional Servers&lt;br&gt;Identity Data Integration</td>
<td>NDC/Center Trust Relationship Desirable&lt;br&gt;IdM Deployment&lt;br&gt;IdM Data Integration For Provision Of Verified Identities To CBACS Master And Regions</td>
<td>Send Requested Data Call To Center Management (OSPP And OCIO)</td>
</tr>
<tr>
<td>Physical Access Via One NASA Badge Utilizing E-PACS</td>
<td>Q4FY05</td>
<td>Regional Server Deployment&lt;br&gt;E-PACS Compatible Backend Infrastructure</td>
<td></td>
<td>CBACS -provided E-PACS Training&lt;br&gt;Local Center&lt;br&gt;Compatibility Review With Issues Noted</td>
</tr>
<tr>
<td>Physical Access Via Smart Card One NASA Badge</td>
<td>FY07</td>
<td>Install Medium Assurance Smart Card Readers For Physical Access&lt;br&gt;Install Smart Card Management System</td>
<td>CIMS – Enterprise LDAP Directory</td>
<td>Smart Card Badge Issuance Training&lt;br&gt;Local Center&lt;br&gt;Infrastructure Upgrade To New Readers</td>
</tr>
<tr>
<td>Logical Access Via Smart Card One NASA Badge</td>
<td>FY07</td>
<td>Deploy Middleware For All Users&lt;br&gt;Deploy Readers For All Users</td>
<td>PKI Integration</td>
<td>Coordinate With Desktop Providers</td>
</tr>
</tbody>
</table>
### Critical Project Risks

- Requirements gaps of current COTS products and scheduled releases
- Availability of new technology contactless readers
- Issuance of non-waiverable FIPS 201 and associated NIST SP 800-73, which define Federal standards
- Approach for compliance with NIST identity standards in response to HSPD-12, including such capabilities as biometrics
- Establishment of consistent business processes and procedures
- Establishment of standards for Regional and Enterprise PACS
- Definition and design of CM processes for updating E-PACS database fields and forms after implementation
- Provision of identity data for the E-PACS and IDMS
- Replacement of existing physical readers
- NASA’s final card buy
- Projects currently underway
## CBACS - Planning Approach

<table>
<thead>
<tr>
<th>New Work Planning Documents</th>
<th>Compliance</th>
<th>Reason for not complying or N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMB Circular A-11 – Business Plan</td>
<td>Complies</td>
<td></td>
</tr>
<tr>
<td>NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems</td>
<td>Complies</td>
<td></td>
</tr>
<tr>
<td>NIST Special Publication 800-18, Guide for Developing Security Plans for Information Systems</td>
<td>Complies</td>
<td></td>
</tr>
<tr>
<td>NPR 7120.5C, Sections 3.2, 3.4 3.5.2, and 3.5.3</td>
<td>Will Comply</td>
<td>Evaluation underway to ensure compliance</td>
</tr>
<tr>
<td>NPD 8710.1, Emergency Preparedness Programs</td>
<td>Complies</td>
<td></td>
</tr>
<tr>
<td>NPR 1620.1, Security Procedures and Guidelines</td>
<td>Complies</td>
<td></td>
</tr>
<tr>
<td>NPR 2810.1 Security of Information Technologies</td>
<td>Complies</td>
<td></td>
</tr>
<tr>
<td>NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems</td>
<td>Final Evaluation Underway</td>
<td></td>
</tr>
<tr>
<td>NPR 7150.2, NASA Software Engineering Requirements, and NASA Standard 8739.8, Software Assurance Standard</td>
<td>Will Comply</td>
<td>Evaluation underway to ensure compliance</td>
</tr>
</tbody>
</table>
Next Steps

- Complete Regional Server and Workstation connectivity
- Receive Authority To Operate (ATO) for current environment
  - CBACS independent audit began September 11 for C&A in preparation to receive and authority to operate. Final report pending
  - First HIGH to be evaluated using NIST 800-53 controls
- Compete Center-specific requirements
- Initiate Smart Card activities to meet HSPD-12 deadlines
- Updated CBACS Security Plan – NIST 800-18
- Update CBACS Risk Assessment Plan -- NIST 800-30
- Complete final design documents
- Stage, configure and test CCMS Server
- Conduct Smart Card Key Ceremony
- Refine communications and change management strategies
- Conduct CDR milestone review
Summary - Why CBACS?

- One view of badging and access control
- One system to certify
- One system to secure
- One system to ruggadize
- One system to upgrade
- One system to measure
- One system to provide better information and shared services
- Re-alignment of workforce to be customer facing
- Processors are cheap - but these are not:
  - Space
  - Power
  - Installation
  - Configuration
  - Administration
  - Integration
  - Global Policies
  - Maintenance
  - Patching
  - Upgrades

Reduce, consolidate, scale, and partner!
NASA began a Smart Card implementation in January 2004. Following site surveys, it was determined that NASA's badging and access control systems required upgrades to common infrastructure in order to provide flexibly, usability, and return on investment prior to a smart card implantation. CBACS provides the common infrastructure from which FIPS-201 compliant processes, systems, and credentials can be developed and used.