Interagency Advisory Board

Meeting Agenda, September 27, 2010

1. **Opening Remarks**
2. **Transportation Worker Identity Credential Program Status Update** *(John Schwartz, TWIC PM)*
3. **Virginia First Responder Authentication Credential Status Update** *(Mike McAllister, Virginia Department of Transportation)*
4. **Sanofi-Aventis Implementation of Digital Identity Using SAFE-BioPharma** *(Peter Loupos, VP Prospective and Strategic Initiatives)*
5. **Identity Business Architecture 2.0—Beyond PIV** *(Corinne Irwin, NASA)*
6. **Update on Government Smart Card Training** *(Randy Vanderhoof, Executive Director of the Smart Card Alliance)*
7. **The Difference Between PIV-I and PIV-C** *(Tim Baldridge, NASA)*
8. **Closing Remarks**

National Aeronautics and Space Administration

Beyond PIV:
NASA's Identity Framework 2.0

Corinne Irwin
Corinne.S.Irwin@nasa.gov
Office of the Chief Information Officer

Agenda

- NASA's ICAM Architecture
- Drivers for Identity Framework 2.0
- Identity Framework 2.0
  - » Concepts
  - » Challenges
- Conclusions

Before HSPD-12…

- NASA had initiated several projects prior to HSPD-12
  - » Smartcard Badging and Physical Access Control
  - » Cyber-Identity Management System
  - » NASA Account Management System
  - » eAuthentication project
- When HSPD-12 was signed, we integrated these loosely related projects more tightly
  - » Underwent a non-Advocate Review
  - » Major finding: Develop an enterprise architecture segment

I can...
with ICAM
Identity, Credential, and Access Management

NASA's implementation of Federal ICAM

Identity Management and Account eXchange (IdMAX) – Single Authoritative source of all NASA identities

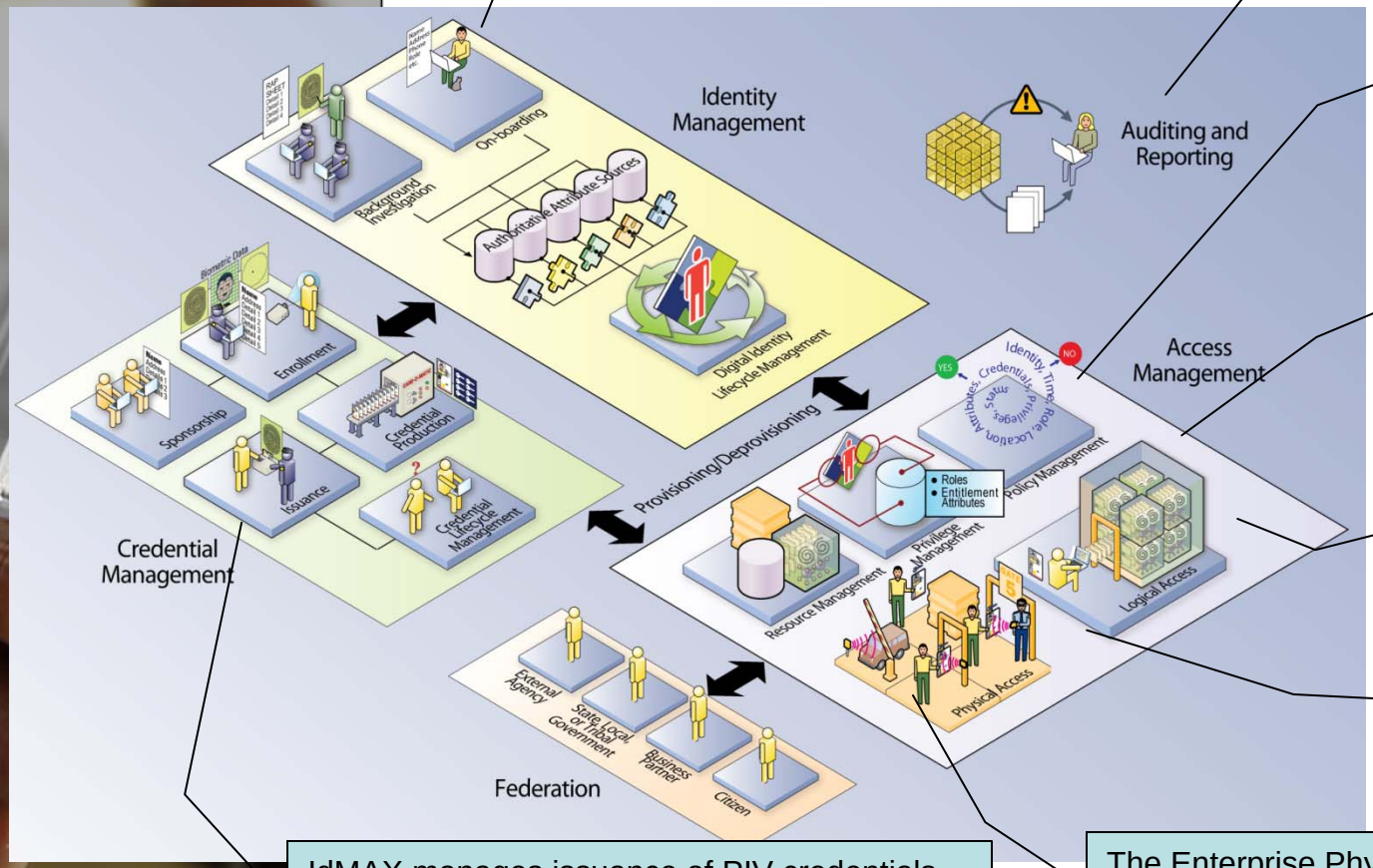
ICAM Audit Viewer allows us to track every change made to a person.

IdMAX manages account request and approval for NASA applications,and automaticall provisions to the Launchpad.

NASA's Consolidated Active Directory (NCAD) controls access to desktops and applications such as e-mail and SharePoint.

The Access Launchpad provides access control for web-based applications.

The Agency RSA infrastructure supports applications that cannot use PIV smartcards.



IdMAX manages issuance of PIV credentials, RSA Tokens, AD accounts, and Launchpad Accounts.

The Enterprise Physical Access Control System (EPACS) controls access to buildings and doors throughout NASA.

ICAM Implementation Status

- Identity Management and Account Exchange (IdMAX)
  - » Single authoritative source of all NASA identities
  - » Contains workflows for PIV Issuance
  - » All other ICAM systems directly tied to IdMAX identities
- Enterprise Physical Access Control System (EPACS)
  - » Operational since 2005
  - » Upgraded to accept PIV smartcards in addition to proximity
- NASA's Consolidated Active Directory (NCAD)
  - » Project Completion Review held May 18, 2010
  - » Smartcard-enabled
- eAuthentication/Launchpad
  - » Operational since 2005
  - » NCAD integration in Spring 2010
  - » Smartcard and RSA integration in Summer 2010
- Agency RSA Consolidation
  - » Center migrations May - November 2010
  - » Smartcard integration early 2011 to support VPN access
- Application Integration Status
  - » 85% of applications integrated with NAMS
  - » 40% of applications integrated with NCAD or Launchpad

Cool Stuff we can do today

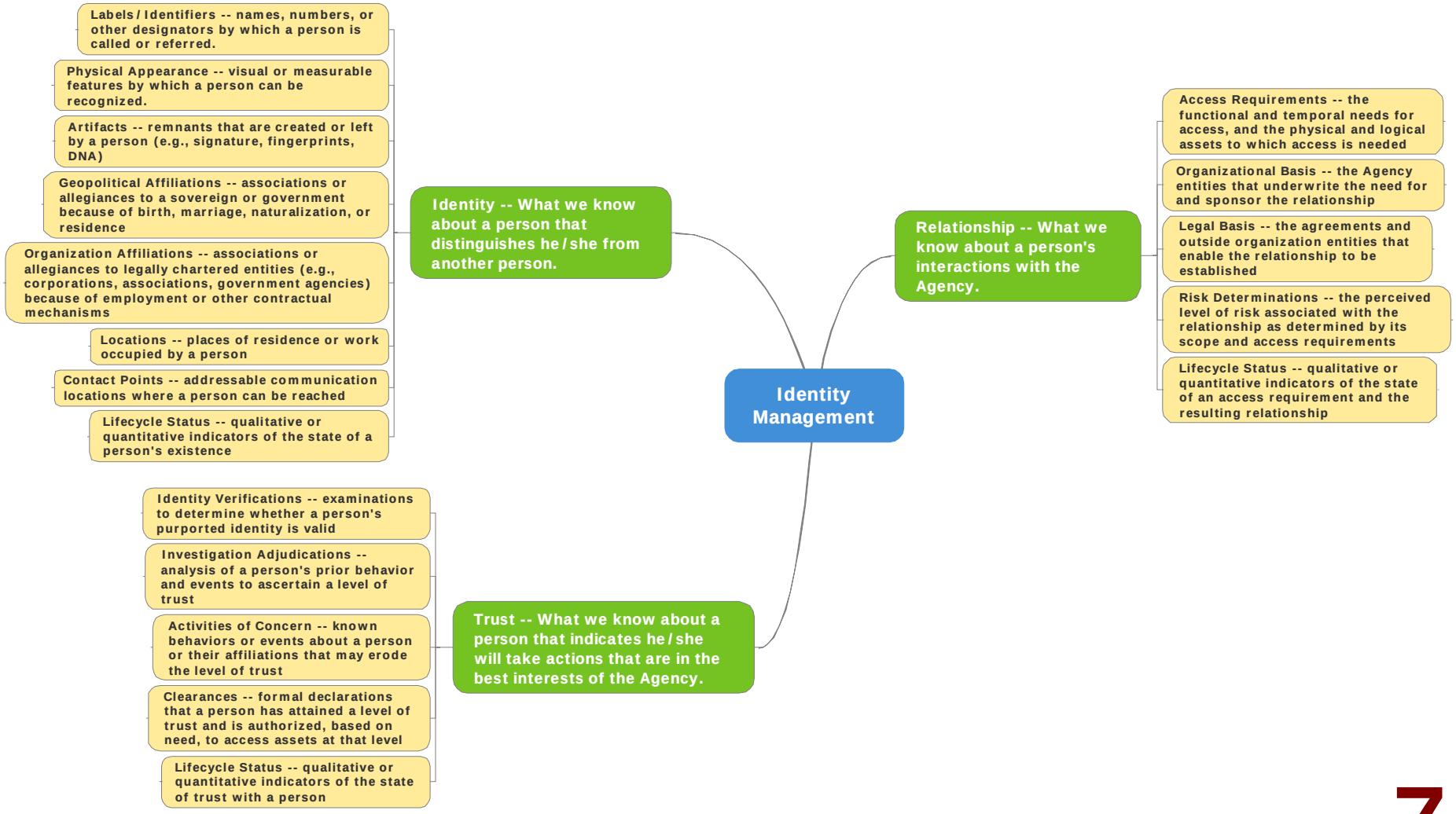
- Smartcard login to the desktop, then get to over 900 applications without re-logging in
- Any NASA worker can visit any NASA Center, and get:
  - » Pre-authorized access to any building/room
  - » Wireless access to the NASA network
- Ensure on a person-by-person basis that those who need IT security training have taken it
- Provide “Basic Level of Entitlement” access to IT systems based on Identity attributes
- Initiate “Close Account” processes on 85% of our IT assets when someone leaves

Drivers for Identity Framework 2.0

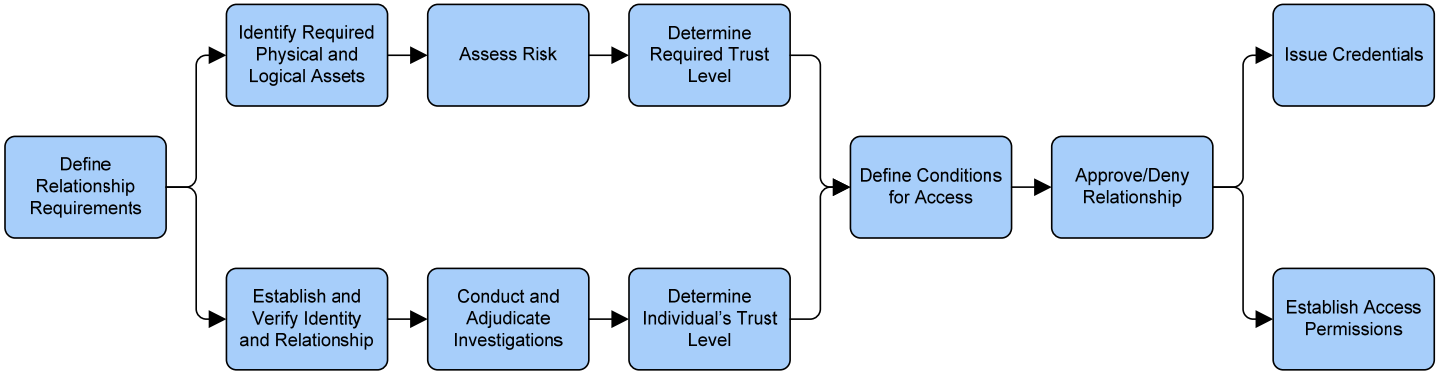
- Identity Framework 2.0 addresses several issues:
  - » Identity processes tied too closely to issuance of a PIV credential
  - » On-boarding issues
  - » Inability to allow for “states” of identities and relationships
- Identity Framework 2.0 supports the future of ICAM:
  - » Incorporates Foreign Nationals and Visitors into ICAM
  - » Accepts Federated Credentials issued by other government and private issuers
  - » Ensures Identity vetting is commensurate with the Level of Risk of access to an asset

I can... with ICAM
Identity, Credential, and Access Management

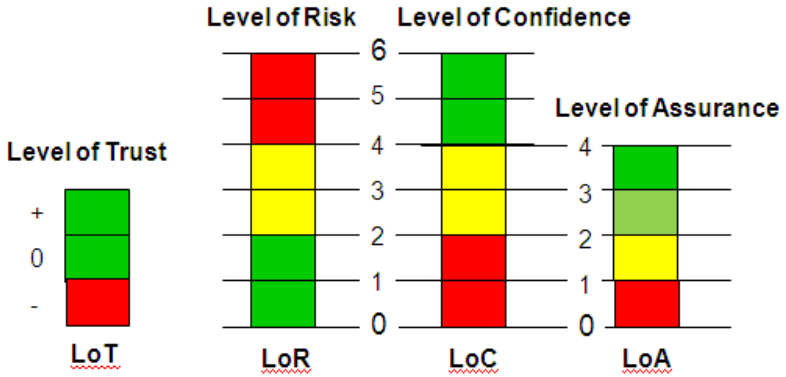
Identity Management Dimensions



Consistent Process



- All scenarios (e.g., new civil servant, remote user, foreign national, public visitor) are handled by a single consistent workflow
- Checklists driven by policies determine which logic paths (series of activities) are required in each activity for each scenario
- A consistent process reduces complexity and the number of workflows – improving consistency and reducing cost



LoT = LoC - LoR

Assets

Level of Risk – the degree of potential damage that access to an asset represents (financial, safety/security, reputation)

People

Level of Confidence – the degree of certainty that a person is who s/he claims to be

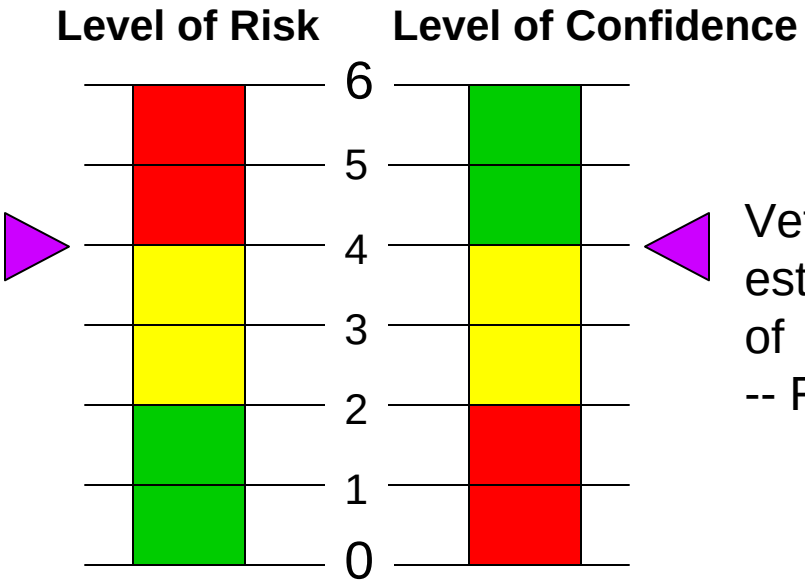
Credentials

Level of Assurance – the degree of certainty that a credential presented represents the person who is accessing the asset

Level of Trust – the degree certainty that a person's access to an asset is an acceptable risk

I can... with ICAM
Identity, Credential, and Access Management

Trusted Relationships



Analysis processes determine level of risk
-- Focus on Access --

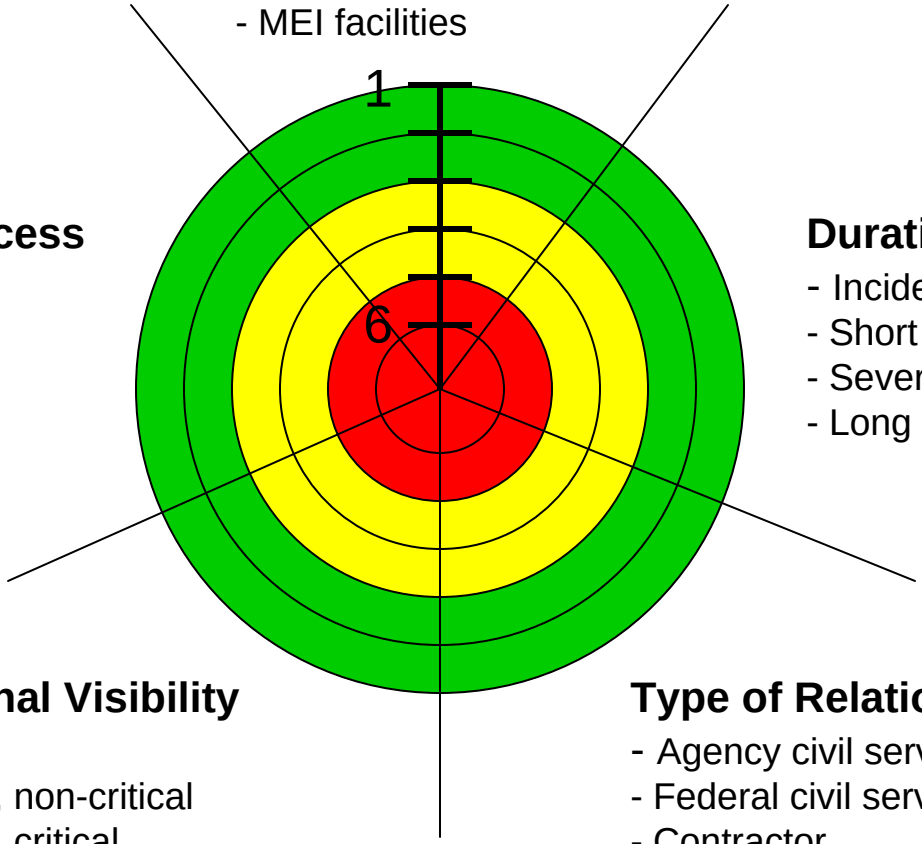
Vetting processes establish level of confidence
-- Focus on Trustee --

- Two independent variables that are dynamic and monitored, and have a consistent scale and can be correlated
- A match indicates a trusted relationship, and the appropriate credentials and permissions may be issued and granted
- A mismatch indicates changes in the relationship to be addressed – especially if level of confidence < level of risk
- Trusted relationships are established with people and groups of people (e.g., organizations, communities)

I can... with ICAM
Identity, Credential, and Access Management

Factors That Establish Risk

Assets Required
- Public areas
- Basic entitlements
- Classified information
- MEI facilities



Locations of Access
- Agency site
- Remote in U.S.
- Remote overseas

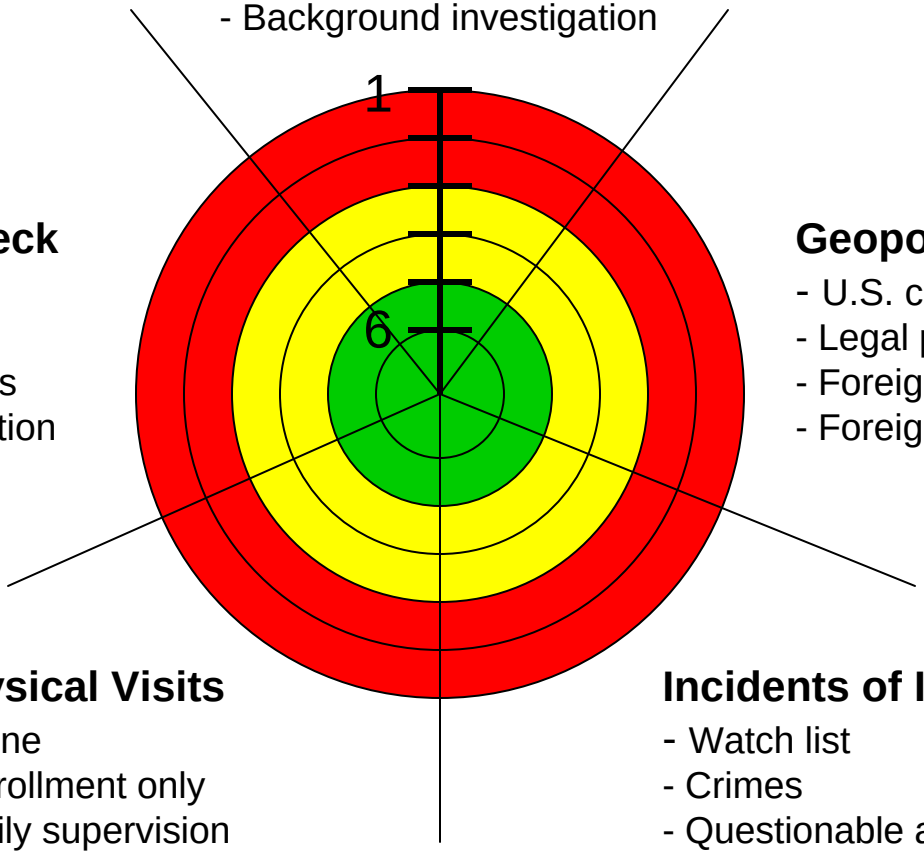
Duration of Access
- Incidental
- Short term
- Several visits
- Long term

External Visibility
- None
- Work, non-critical
- Work, critical
- High level communication

Type of Relationship
- Agency civil servant
- Federal civil servant
- Contractor
- Independent

Factors That Establish Confidence

Investigations
- None
- Database checks
- NACI
- Background investigation



Credentials Check
- None
- Govt issued docs
- Secure credentials
- Database verification

Geopolitical Affiliations
- U.S. citizen
- Legal permanent resident
- Foreign national
- Foreign national designated

Physical Visits
- None
- Enrollment only
- Daily supervision

Incidents of Interest
- Watch list
- Crimes
- Questionable acts
- None

Challenge: Aligning LoR with M-05-24

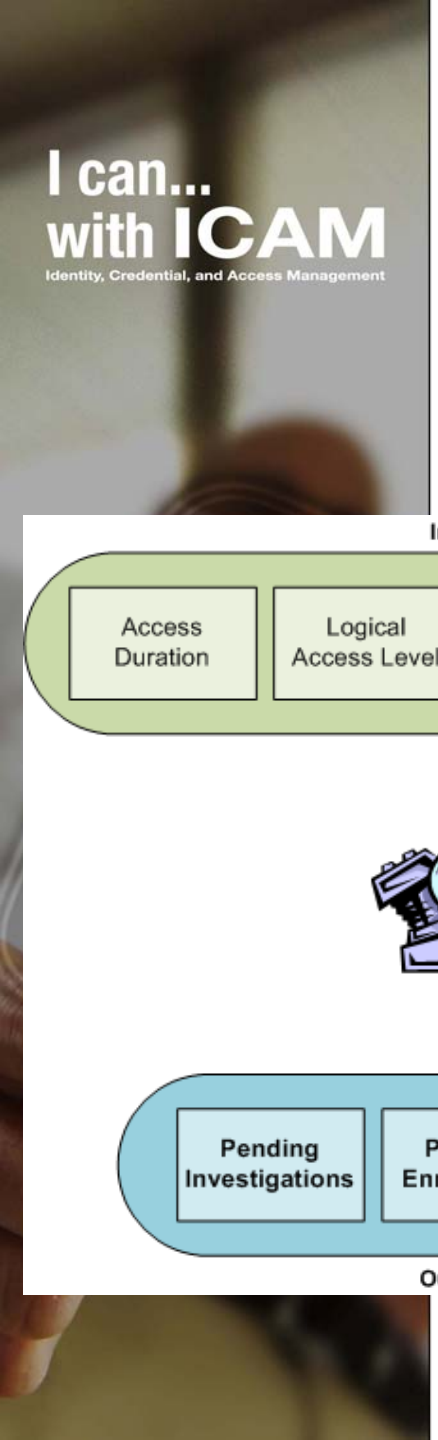
- Per M-05-24, PIV credentials must be issued to employees and contractors who require long-term access to Federally controlled facilities and/or information systems.
- Yet:
  - » A PIV credential assumes “high” LoR
  - » Many civil servants and contractors only have access to “low risk” assets
  - » We let people onto NASA campuses for more than 6 months for carpools, day care pickup, clubs, etc

Challenge: Aligning LoR with M-05-24

- **Assumption 1**: There is a previously unquantified risk due to one or both of the following:
  - » Duration of access to the asset
  - » Aggregate risk from access to multiple assets
- **Assumption 2**: There is higher risk inherent in a “work” affiliation that is not present for “non-work” affiliations

Security Domains

- Four components are measured to determine overall Security Domain required of each identity seeking access to NASA assets:
  - » Physical Access Level of Risk
  - » Logical Access / IT Level of Risk
  - » Physical Access Duration
  - » Assignment Risk
- As LoC increases, overall Security Domain access is allowed
  - » Access to a specific asset within the Security Domain is still dependent on authorization based on need



Identity Logic Engine

The Identity Logic Engine works behind the scenes within IdMAX to create the required outputs so you don't have to!

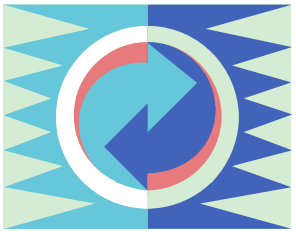
- Inputs:
  - » Levels of Risk as determined when the identity was created / modified
    - Duration (length of affiliation to NASA)
    - Logical (IT) Access
    - Physical Access
    - Assignment Risk (i.e. Public Trust, etc.)
- Outputs:
  - » Appropriate system objects to establish the required Level of Confidence
    - Investigation requests
    - Enrollment requests
    - Credential requests

Challenge: Setting Logical and Physical LoR

- We should set LoR (Physical) and LoR (Logical) based on explicit access to assets, however:
  - » Requestors don't always know this information in total
  - » Without asset grouping, it would be tedious to assign access to assets as part of the affiliation process
- Interim strategy:
  - » Have the Requestor manually set LoR
  - » Begin assigning LoR to asset access (but don't act on the setting yet)
  - » Monitor LoR setting against asset access requested
  - » Implement asset groups to facilitate future setting of LoR

IF 2.0 Lifecycles

- Current Workflow is a Credential focused workflow only
- IF 2.0 has separate lifecycles for:
  - » Identities
  - » Credentials
  - » Investigations
  - » Relationships

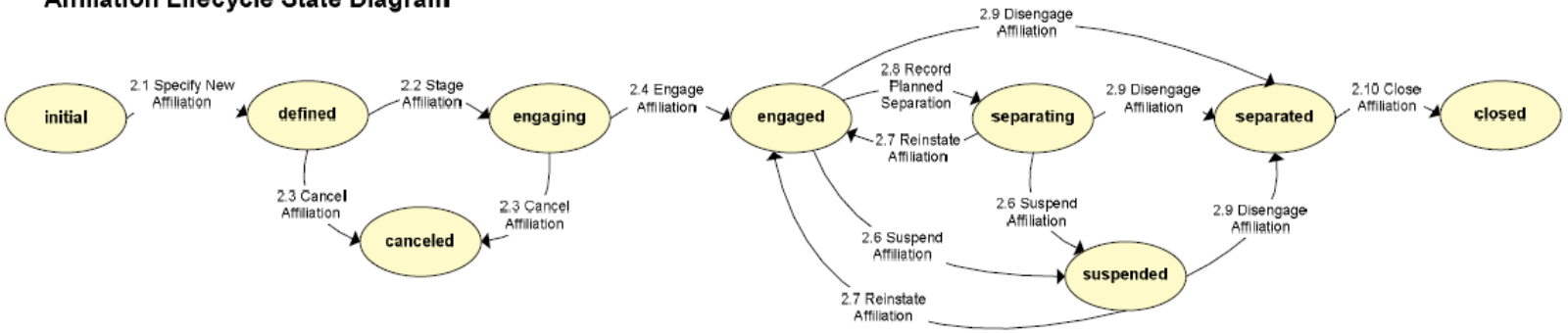


- Benefits:
  - » Change in relationship does not affect status of Identity certainty or investigations
  - » Delays in one of the lifecycles does not necessarily impact the others
  - » A single person can have multiple, concurrent relationships and credentials

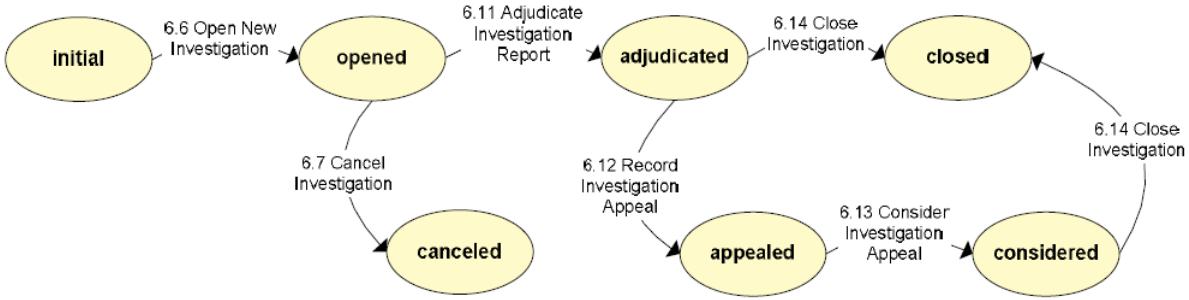
Identity Lifecycle Examples

Person (Claimant) Lifecycle State Diagram

Affiliation Lifecycle State Diagram

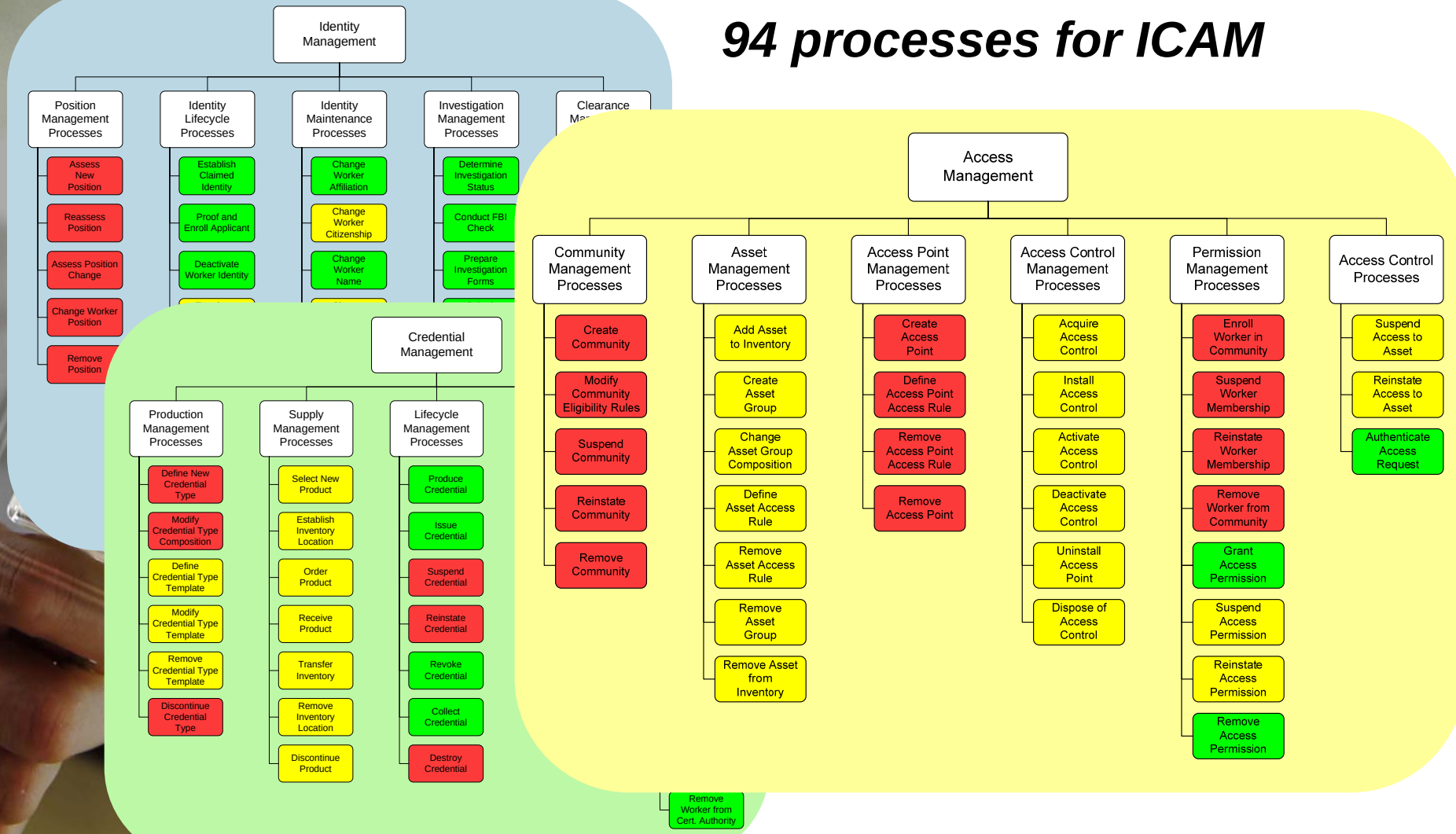


Investigation Lifecycle State Diagram



ICAM v. 1.10 Business Processes

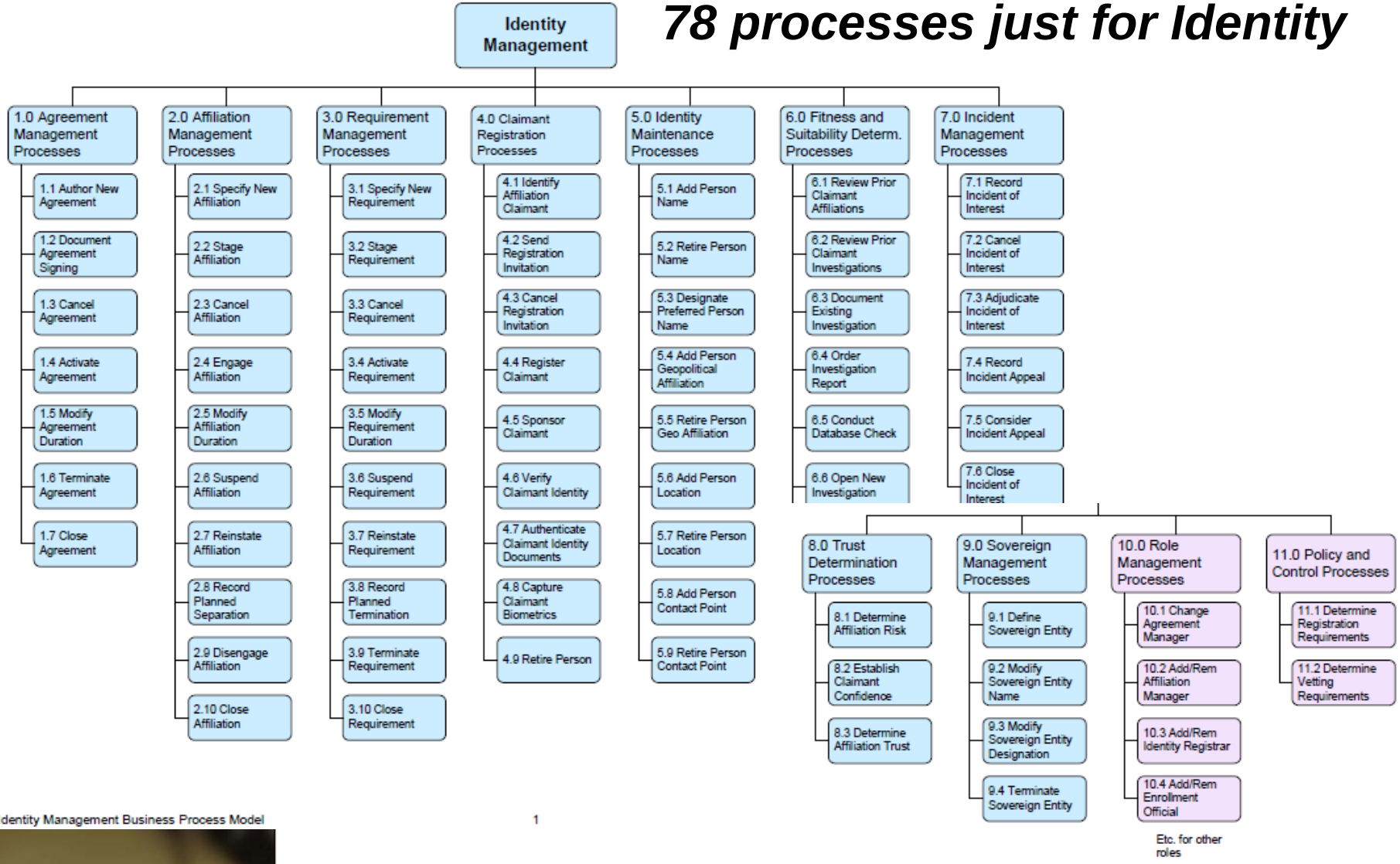
94 processes for ICAM



I can... with ICAM
Identity, Credential, and Access Management

Identity Management 2.0 Processes

78 processes just for Identity



Conclusions

- Identity framework 2.0 matures NASA's architecture to meet needs for:
  - » ICAM beyond PIV smartcard issuance
  - » Lifecycle states for identity, affiliation, and trust
  - » Access decisions based on level of trust
- Quantification of LoR based on aggregation and/or duration of access is a challenge
- Full implementation will be part of our ICAM roadmap
- Next up: Credential Management 2.0!


I can...
with ICAM
Identity, Credential, and Access Management
Vargas, Omar
JAN 2013
NASA

Questions?