Department of the Air Force

DAF Enterprise ICAM

Rick Moon
Chief, Protect Branch
AFLCMC/HNID
2 Jun 2022

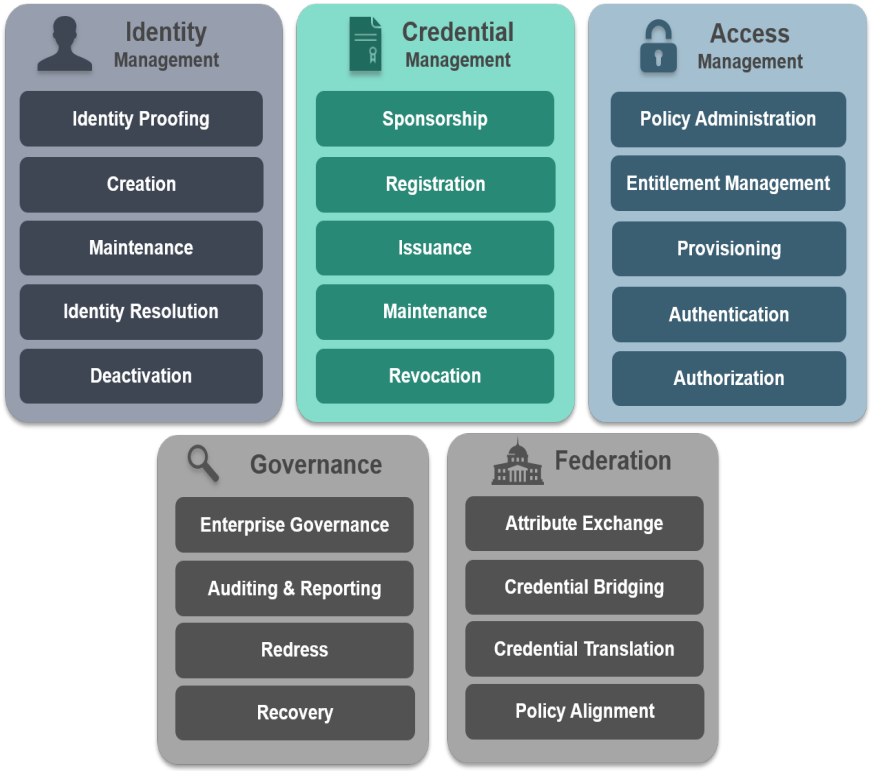
Objectives

- What is ICAM?
- Why ICAM?
- Roadmap
- Lines of Effort
- Way Ahead and Wrap Up
- Questions

What is ICAM?

ICAM

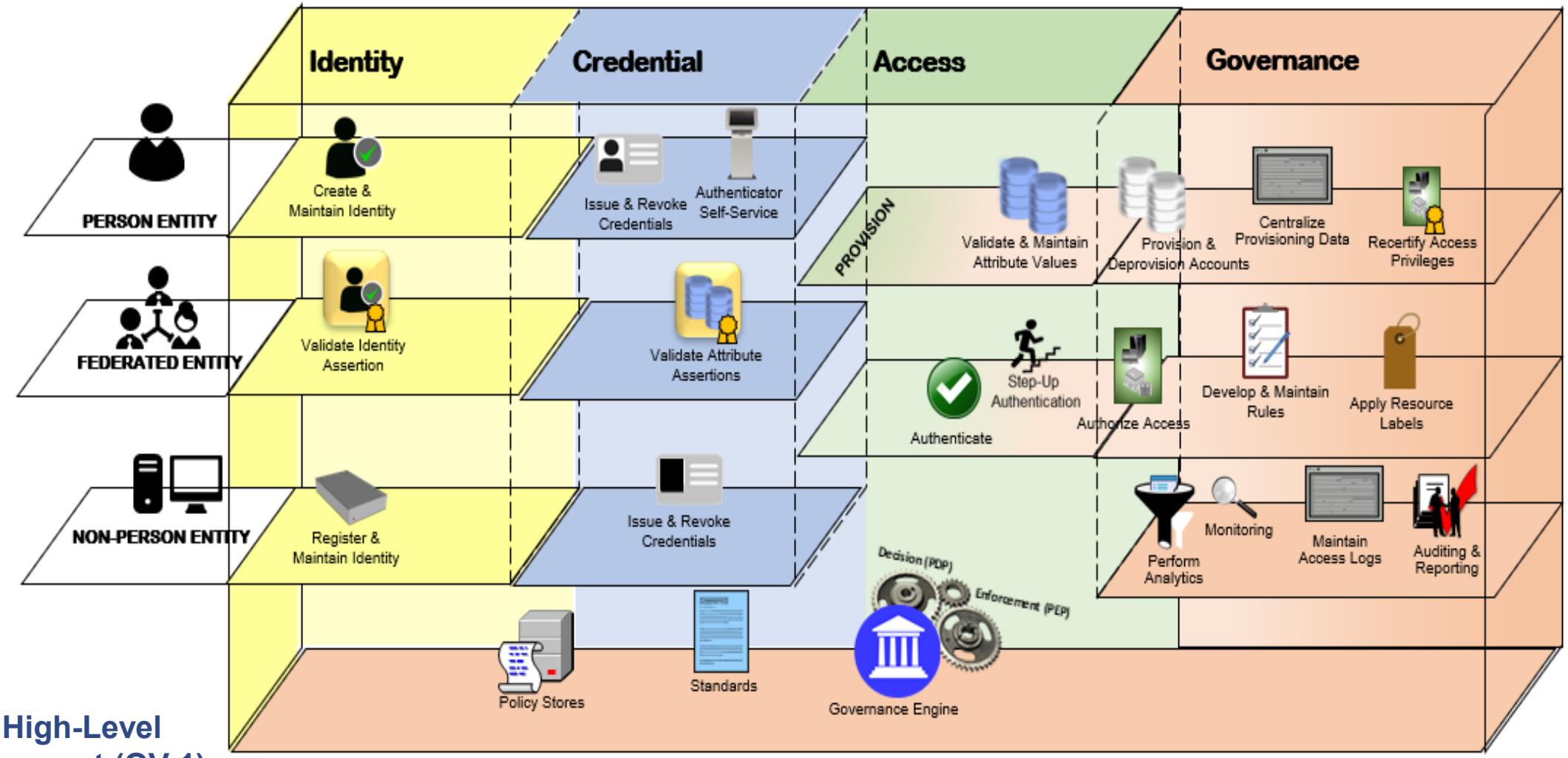
- **What Is ICAM?**
  "the set of security disciplines that allows an organization to enable the right individual to access the right resource at the right time for the right reason"[1]
- **Main Components**
  - **Identity Management**
  - **Credential Management**
  - **Access Management**
- **Supporting Functions**
  - **Governance**
  - **Federation**



[1] – *Federal ICAM Architecture*

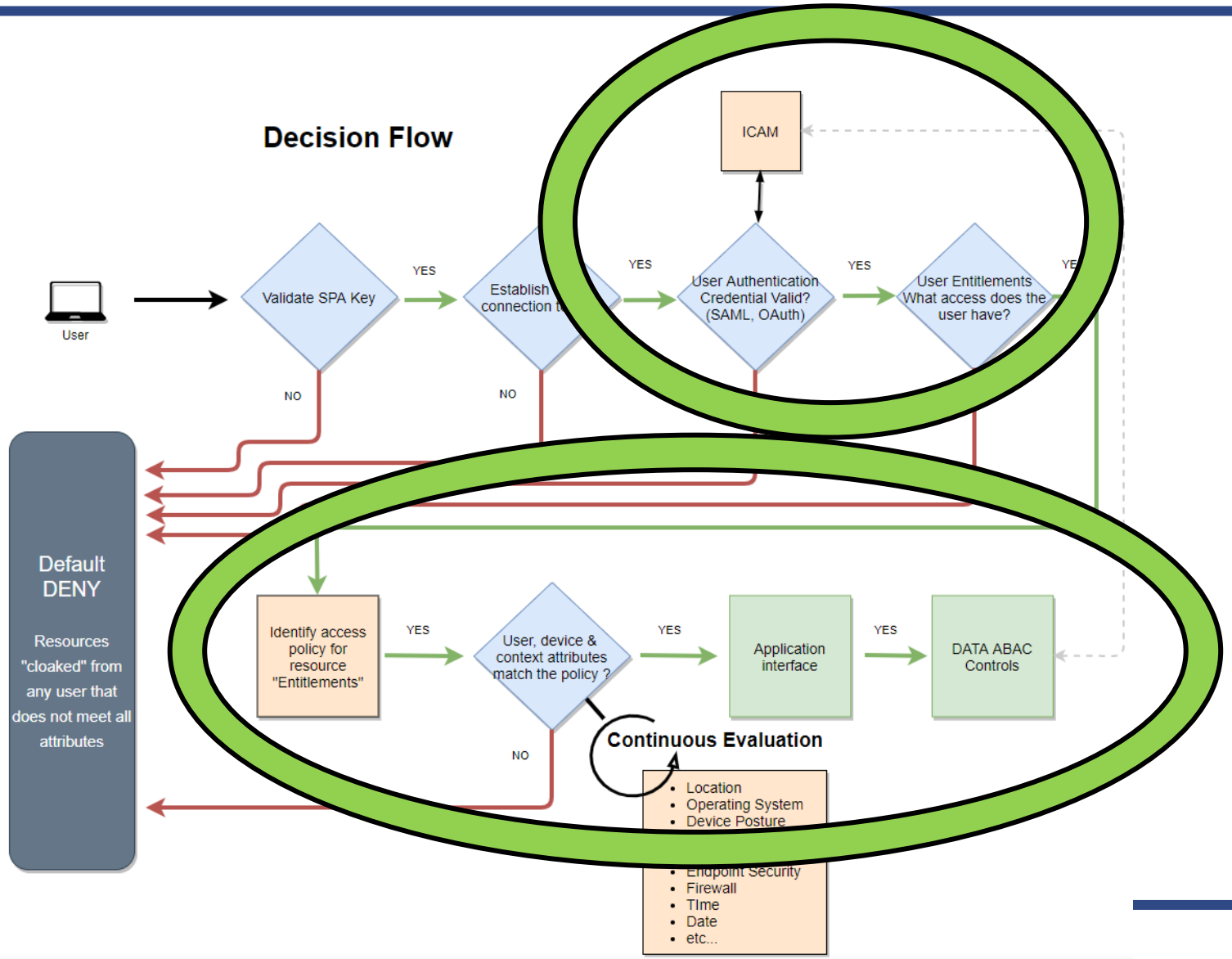
Picture Source: https://arch.idmanagement.gov/services//

DAF ICAM OV1



DAF ICAM High-Level Operational Concept (OV-1)

ICAM in the Zero Trust Decision Flow



Why ICAM?

The Burning Platform Problem

The Burning Platform

- **Audit findings related to access management/ security still common**
  - ***Individuals escalating their own privileges***
  - ***Duty separation not tracked***
  - ***User access/privileges not changed when warranted***

Current State

- **IDs managed by each application of systems creating identity silos**
- **Poor account management**
  - **Access based on manual process**
  - **Non-standard access deletion process resulting in cyber security issues for personnel no longer requiring access**
- **More than 2875/577 workflow *(e.g., privileges, SOD, privileged escalation, audits)***

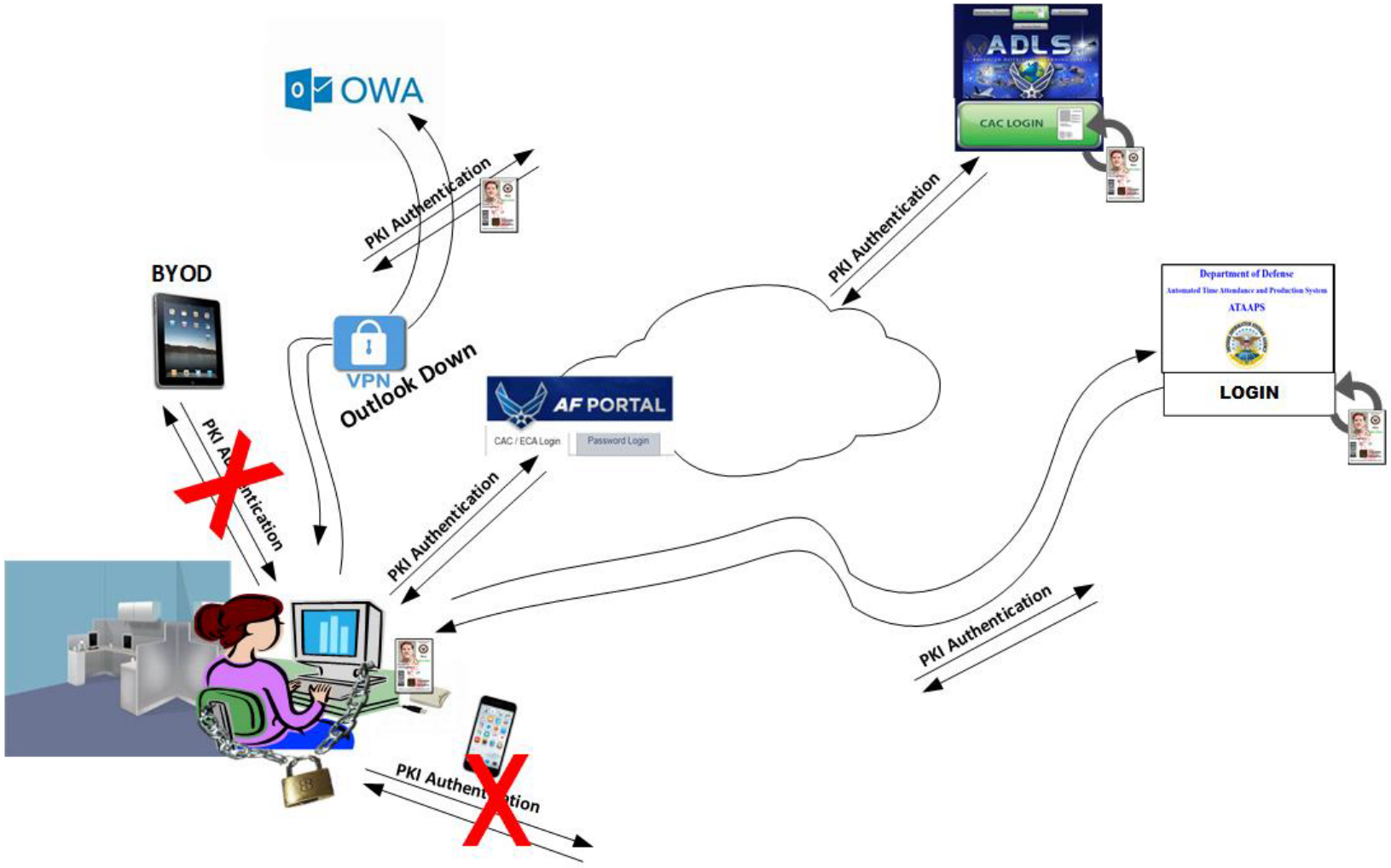
Recommendation

- **Establish a centralized identity platform that automatically manages user's access to apps**

Benefits

1. **Enhanced user experience**
2. **Reduced Manual Operator Workload**
3. **Improved cybersecurity with foundation for ZT**

Current Environment



Future State

DAF ICAM Strategy & Capabilities

Goal 1: Centralized Identity Management

- Automate DD Form 2875 process
- Increase AFID delivery of identity data to AF functional areas
- Assign identity attributes to NPEs
- Provide reciprocal access to system resources between DAF and mission partners

Goal 2: Universal Authenticator Support

- Use CAC to enable authenticators for use in situations where CAC is not practical or available *(e.g., retirees, dependents)*
- Integrate commercial solutions into web/app-based authentication

Goal 3: Seamless Enterprise Access Management Services

- Create ABAC-enabled enterprise dynamic authorization framework
- Automate provision/de-provision processes
- Enhance existing SIEM capabilities to drive out anonymity across DAF enterprise networks

Goal 4: Standardized DAF ICAM Governance Framework & Policy Enforcement

- Establish AF focal point for Service/Agency gps
- Create policies for standardized deployment of ICAM technologies
- Vet & analyze requirements for ICAM capabilities
- Work with SAF/CDO on policy for auto data tag

DAF Enterprise ICAM Design Criteria

- **User Population Includes:**
  - **Person**
    - **CAC holders**
    - **Non-CAC holders**
    - **Daily Users**
    - **Non-Daily Users**
    - **Subpopulations with multiple personas**
  - **Non-Persons**
    - **Devices**
    - **RPAs**
- **DAF solution must support segmented environments**
  - **NIPR closed enclaves with the same tech stack and segmented user base**
  - **SIPR with the same tech stack and segmented user base**
- **Non-PKI Authenticator Support**
  - **Support for non-CAC holder user population**
- **Multiple competing priorities for scheduling system migration**
  - **FIAR relevant systems – CPG guidance**
  - **Zero Trust**
  - **Mission systems – DoD**

ICAM Roadmap

SAF/CN ROADMAPS DEEP DIVE | *ICAM Background*

Identity Credential and Access Management will provide foundations for who you are and what you have access to.

Why is it important?

Centralized identity is one of the most critical components for IT security. It centralizes our authorization (what you can access) to provide least privilege and excellent auditability to meet our FIAR responsibilities.

How does it deter our adversaries?

With standards-driven enterprise control we set a foundation for our Zero Trust architectures and prevent flawed implementations. It extends to all classification levels and makes it easier to work with other services and allies.

Funding Assessment

Partially funded in FY22, fully funded in FY23-FY25

Ownership

HNI

SAF/CN (EIT Portfolio)
ACC (Lead Command)
16AF (Operator)
CCC (Requirements)
HNID (Acquisition)

Collaboration/Stakeholders:
PlatformOne, CloudOne, A1, SAF/FM, DAF365, EITaaS, etc.

Phase of Maturity

Pilots →

Key Challenges

- Onboarding of thousands of applications that require small to medium code changes and hardening
- Navigating the stated desires of the DoD to create a centralized service

Next Steps

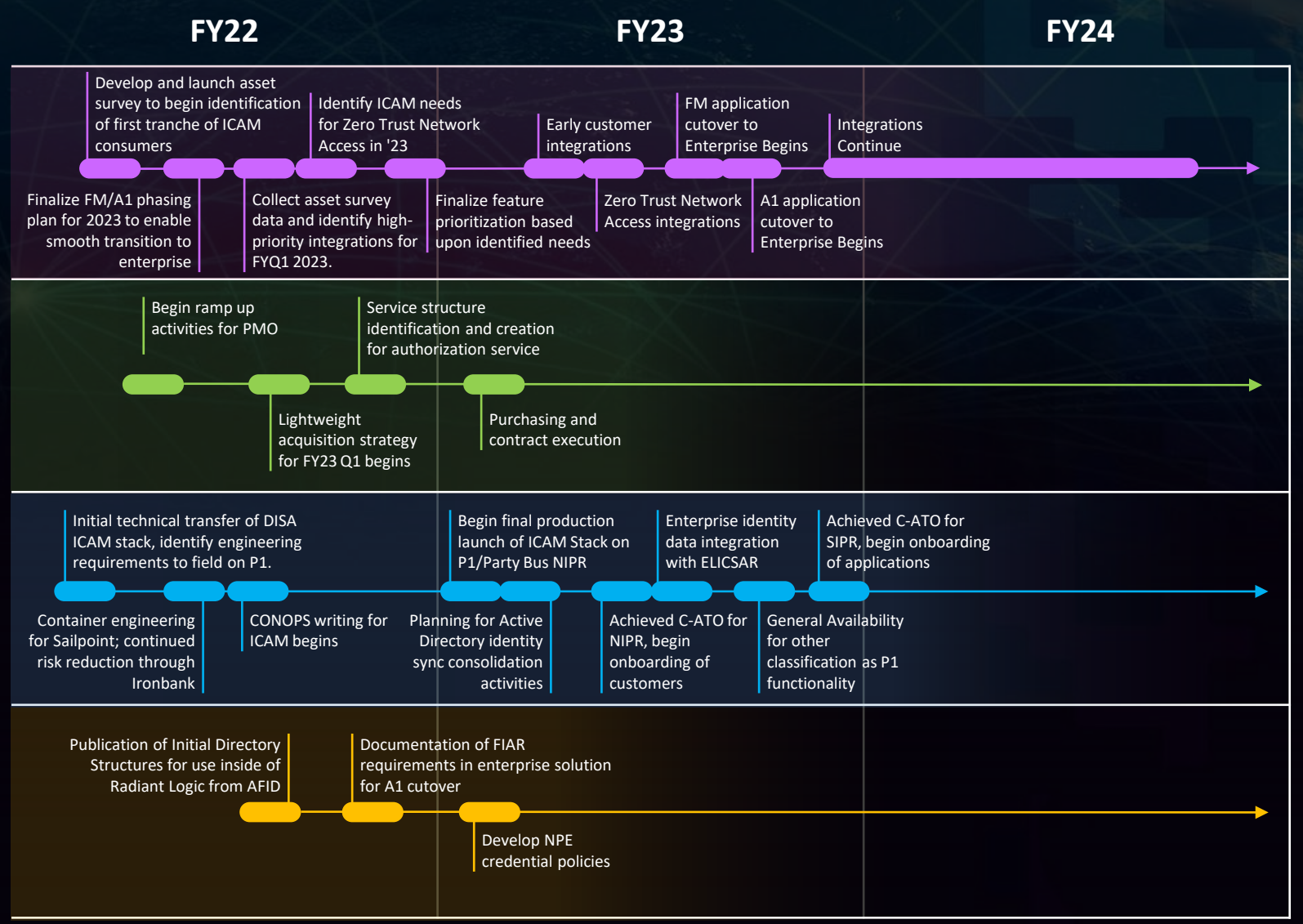
- Set up ICAM program office to manage deployment
- PlatformOne engineering work in ‘22
- ICAM CONOPS writing (in progress)
- Ongoing engineering work with P1

Pacing:

- Operational capability by Q2FY23; ICAM CONOPS delivery Q3FY22

SAF/CN ROADMAPS DEEP DIVE | *ICAM Sub-Roadmap*

The timeline below outlines the ICAM approach over the next three fiscal years.



SUCCESS IN FY22

Identify integration on-ramps for ‘23

- ❑ Understand portfolio of applications and initial adopters *(shared with Zero Trust)*
- ❑ ICAM deployment to PlatformOne
- ❑ Bridge A1/FM efforts to support FIAR into ‘23

DAF Enterprise ICAM Lines of Effort

AF ICAM Lines of Effort

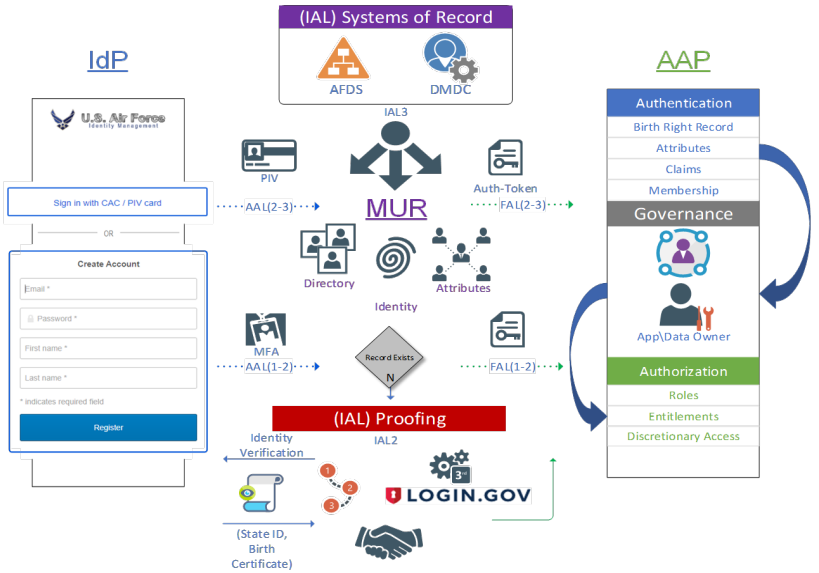
- **AF has 3 ICAM LOEs driving to a singular enterprise solution:**
  - **LOE 1: ZT pilot support**
  - **LOE 2: FIAR System A1 Effort**
  - **LOE 3: Enterprise ICAM Pathfinder**

LOE 1: ZT Pilots

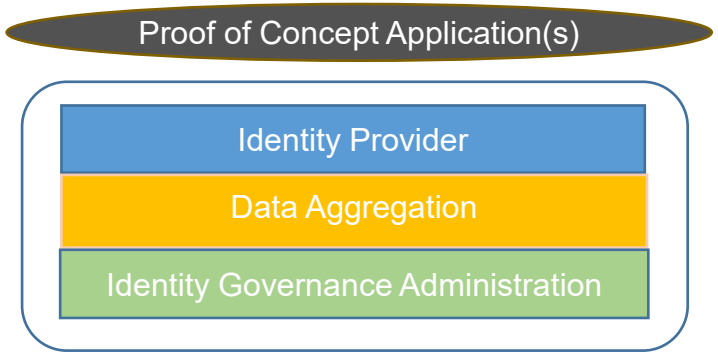
- Providing identity and Access Management support
- Each pilot slightly different
- Solutions based on desired outcome for each pilot
- Includes:
  1) Cape Canaveral
  2) Hickham AFB
  3) Beale AFB

LOE 2: FIAR System A1 Effort

Working with SAF/FM & A1 to onboard audit relevant systems to A1 ICAM platform until DAF enterprise is operational



LOE 3 : Enterprise ICAM Pathfinder Stack



Pathfinder helps drive architecture decisions for end state enterprise ICAM

ICAM Pathfinder

Capability	Objectives	ICAM Pathfinder Expected Outcomes
Identity Provider & Authentication Mgmt	**1. User Data Ingestion & Provisioning** **2. Context-Aware General User Access**	1. Connect to authoritative source for user's "birth right" attributes to the directory 2. User redirected to IDP via browser header upon login attempt; once successfully authenticated, user granted access if they meet established requirements
Attribute Aggregation	**1. Identity Attribute Repository** **2. Integration**	1. Connect to data source for updating users and associated attributes to the directory 2. Demonstrate a simple application that queries the IDP via IGA; provides authorization token for user
Identity Governance & Administration	**1. De-provisioning** **2. Identity Governance & Administration (IGA) Services** **3. Reporting**	1. Automated action based on changes in attributes and resource application rules 2. Repository for birth-right entitlement and access policies set by resource owners 3. Store auditing & logging information for centralized reporting

Way Ahead and Wrap Up

DAF Enterprise ICAM Way Ahead

- **Near Term**
  - **Working the Pathfinder(s) to realize demonstrable capability**
  - **Collaborate with stakeholders to onboard ICOFR systems to A1 ICAM capability until DAF Enterprise is available**
  - **Working AQ Strategy and planning for FY23**
  - **ICAM CONOPS out for formal coordination**
- **Long Term**
  - **Execute FY23 POM funding for DAF Enterprise ICAM**
  - **Begin migration of A1 and remaining audit relevant systems to DAF Enterprise ICAM when capability is operational**
  - **Containerize DAF Enterprise ICAM for the DevSecOps environment**

Questions?