DAF ENTERPRISE ICAM ROADMAP 2.0
INTRODUCTION

BACKGROUND

The DAF Enterprise faces communication disruption, wide cyber exposure to all aspects of operations, and increasingly sophisticated adversaries. **The current technological environment of disparate and siloed solutions further complicates the implementation** of a comprehensive Enterprise ICAM solution.

The Enterprise ICAM Roadmap 2.0 and all other Roadmaps published by the office of the DAF CIO are developed to encourage collaboration between user communities and the Enterprise – **driving accountability and completion of capability objectives.**

A unified Enterprise ICAM solution provides convenient, automated access determinations, risk-based and behavioral-based dynamic access, and enhanced auditability across the DAF.

ENTERPRISE ICAM ROADMAP 2.0 INTENT

- The Enterprise ICAM Roadmap 1.0 (published FEB 2023) was created to drive execution community progress on a comprehensive Implementation Plan by laying out the strategic vision for Enterprise ICAM over the next 3-5 years.

- After a little more than a year since the original publication of the Enterprise ICAM Roadmap 1.0, the **ICAM capability development and production stakeholders (ICAM PEO) have made significant progress along the implementation journey** and SAF/CN sought to visualize the reality of their progress and way forward.

- As a more accurate, real-time depiction of the Enterprise ICAM stand up, **Roadmap 2.0 was recontextualized for the consumer,** displaying the Enterprise ICAM technical narrative with a heavy focus on user community integration.

ESTABLISH ENTERPRISE ICAM SOLUTION

- **Enumerate the tasks and timeline** related to standing up the Enterprise ICAM solution based on real-time updates from stakeholders involved in implementation and execution.

ENABLE ENTERPRISE ICAM SOLUTION SCALE

- Depict strategic-level activities that will **prepare the Enterprise ICAM solution for future enhancements**, modernizations and integrations after initial production and implementation.

INTEGRATE USER COMMUNITIES

- Display **notional timelines** to prompt future environment integrations and migrations, as well as highlight decision points needed plan and execute user community activity.

PROCESS & COLLABORATORS

- SAF/CN **worked directly with the Enterprise ICAM Program Execution Office (PEO)** out of HNID and **SAF/FM ICAM FIAR integration team** to summarize current state development and production tasks into a strategic, technical narrative for the Enterprise stand up.

- This incorporation of current Implementation Plans **verified task alignment and consensus of the plan** across stakeholders.

- **The 2.0 version of the Roadmap includes key strategic activities referenced in Roadmap 1.0** that are critical to driving solution scale post-production. **User community integration timelines are meant to encourage dependent decision points** and integration planning.

MOVING FORWARD

- **Quarterly updates to the Enterprise ICAM Roadmap will remain more accurate following the release of 2.0** given the improved alignment to current state Implementation Plans.
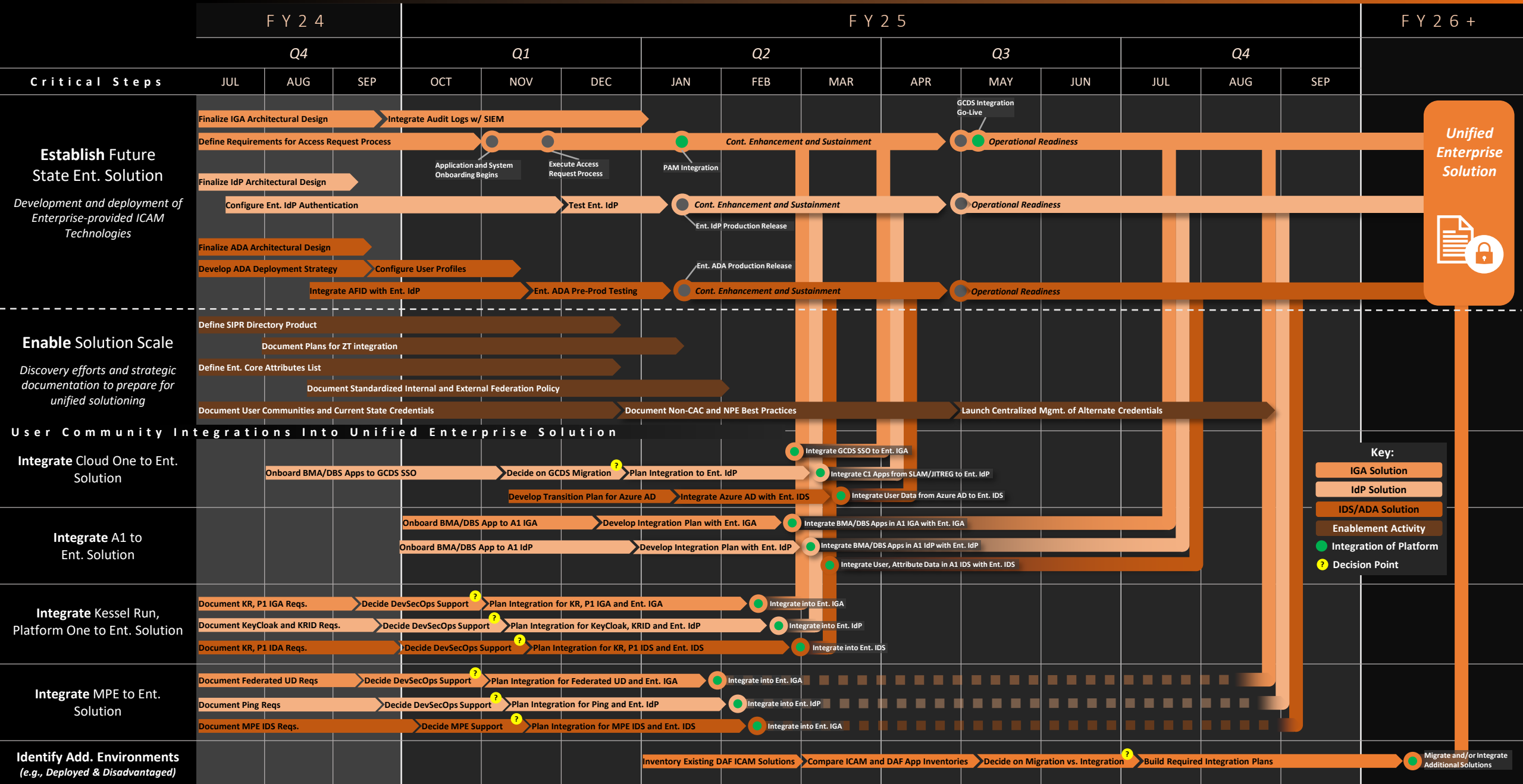
DAF ENTERPRISE ICAM ROADMAP 2.0

	FY24			FY25													FY26+
	Q4			*Q1*			*Q2*			*Q3*			*Q4*			
Critical Steps	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	

Establish Future State Ent. Solution

Development and deployment of Enterprise-provided ICAM Technologies

- Finalize IGA Architectural Design
- Integrate Audit Logs w/ SIEM
- Define Requirements for Access Request Process
- Application and System Onboarding Begins
- Execute Access Request Process
- PAM Integration
- Cont. Enhancement and Sustainment
- GCDS Integration Go-Live
- Operational Readiness
- Finalize IdP Architectural Design
- Configure Ent. IdP Authentication
- Test Ent. IdP
- Ent. IdP Production Release
- Cont. Enhancement and Sustainment
- Operational Readiness
- Finalize ADA Architectural Design
- Develop ADA Deployment Strategy
- Configure User Profiles
- Ent. ADA Production Release
- Integrate AFID with Ent. IdP
- Ent. ADA Pre-Prod Testing
- Cont. Enhancement and Sustainment
- Operational Readiness

Enable Solution Scale

Discovery efforts and strategic documentation to prepare for unified solutioning

- Define SIPR Directory Product
- Document Plans for ZT integration
- Define Ent. Core Attributes List
- Document Standardized Internal and External Federation Policy
- Document User Communities and Current State Credentials
- Document Non-CAC and NPE Best Practices
- Launch Centralized Mgmt. of Alternate Credentials

User Community Integrations Into Unified Enterprise Solution

Integrate Cloud One to Ent. Solution

- Integrate GCDS SSO to Ent. IGA
- Onboard BMA/DBS Apps to GCDS SSO
- Decide on GCDS Migration
- Plan Integration to Ent. IdP
- Integrate C1 Apps from SLAM/JITREG to Ent. IdP
- Develop Transition Plan for Azure AD
- Integrate Azure AD with Ent. IDS
- Integrate User Data from Azure AD to Ent. IDS

Integrate A1 to Ent. Solution

- Onboard BMA/DBS App to A1 IGA
- Develop Integration Plan with Ent. IGA
- Integrate BMA/DBS Apps in A1 IGA with Ent. IGA
- Onboard BMA/DBS App to A1 IdP
- Develop Integration Plan with Ent. IdP
- Integrate BMA/DBS Apps in A1 IdP with Ent. IdP
- Integrate User, Attribute Data in A1 IDS with Ent. IDS

Integrate Kessel Run, Platform One to Ent. Solution

- Document KR, P1 IGA Reqs.
- Decide DevSecOps Support
- Plan Integration for KR, P1 IGA and Ent. IGA
- Integrate into Ent. IGA
- Document KeyCloak and KRID Reqs.
- Decide DevSecOps Support
- Plan Integration for KeyCloak, KRID and Ent. IdP
- Integrate into Ent. IdP
- Document KR, P1 IDA Reqs.
- Decide DevSecOps Support
- Plan Integration for KR, P1 IDS and Ent. IDS
- Integrate into Ent. IDS

Integrate MPE to Ent. Solution

- Document Federated UD Reqs.
- Decide DevSecOps Support
- Plan Integration for Federated UD and Ent. IGA
- Integrate into Ent. IGA
- Document Ping Reqs.
- Decide DevSecOps Support
- Plan Integration for Ping and Ent. IdP
- Integrate into Ent. IdP
- Document MPE IDS Reqs.
- Decide MPE Support
- Plan Integration for MPE IDS and Ent. IDS
- Integrate into Ent. IGA

Identify Add. Environments (e.g., Deployed & Disadvantaged)

- Inventory Existing DAF ICAM Solutions
- Compare ICAM and DAF App Inventories
- Decide on Migration vs. Integration
- Build Required Integration Plans
- Migrate and/or Integrate Additional Solutions

Unified Enterprise Solution

Key:
- IGA Solution
- IdP Solution
- IDS/ADA Solution
- Enablement Activity
- Integration of Platform
- Decision Point

Acronym/Term	Definition
ABAC	Attribute Based Access Control
AD	Active Directory
ADA	API and Data Access
AFID	Air Force Identity
BMA	Business Mission Area
C1	Cloud One
CAC	Common Access Card
DAF	Department of the Air Force
DBS	Defense Business Systems
DevSecOps	Development, Security, and Operations
GCDS	Global Content Delivery System
ICAM	Identity, Credential, and Access Management
IdP	Identity Provider
IDS	Identity Data Service
IGA	Identity Governance and Administration
JITREG	Just In Time Registration
KR	Kessel Run
KRID	Kessel Run Identity
MFA	Multi Factor Authentication

Acronym/Term	Definition
MPE	Mission Partner Environment
NIPR	Non-secure Internet Protocol Router
NPE	Non-Person Entity
P1	Platform One
PAM	Privileged Access Management
SIEM	Security Information and Event Management
SIPR	Secure Internet Protocol Router
SLAM	Simple Lightweight Access Manager
SSO	Single Sign-On
UD	Universal Directory
ZT	Zero Trust