Army Identity and Access Management (IdAM)

3 APR 18

Sergio Alvarez

Product Lead Enterprise Content Collaboration and Messaging (EC2M)

703-704-3788

sergio.m.alvarez.civ@mail.mil

Purpose and Vision

Purpose:

Provide Industry with awareness of the Government's need to transform the Army IdAM capability to an enterprise cloud IdAM capability solution for the US Army and to gather feedback that will assist with the development of an appropriate Performance Work Statement (PWS).

Vision:

To achieve enterprise Identity and Access Management (IdAM) capabilities within a modern framework. The Army's goal for IdAM is to provide a service extensible to all Army and DoD applications, regardless of system configuration or hosting location.

Background: Evolution of IdAM

Today Army IdAM processes and capabilities reside across 3 different states.

Standalone	Army-Centric	DoD-Centric and Army-enabled *(Desired End-state)*
Multiple identities and processes; no central management of users	Single Army digital identity; Central management of Army users across Army IT resources	Single unique DoD digital identity; Central management of DoD users across the Army IT resources
Stove-pipe systems and processes	Army Enterprise Systems (i.e. Army Unified Capabilities)	Army & DoD Enterprise Systems (i.e. DEE, Army UC, DEOS, etc)
Fragmented networks	Limited Army seamless network	Seamless DoD network
No interoperability for collaboration & information sharing	Interoperability across Army; No interoperability across DoD	Full interoperability across DoD enterprise to the tactical edge
Access is granted by Admin	Access granted by groups or local attributes	Access is based on enterprise and Army attributes along with roles

*IdAM is the critical **"Enabling Capability"** that provides seamless, secure, and interoperable network – **Goal is to be DoD Centric and Army Enabled***
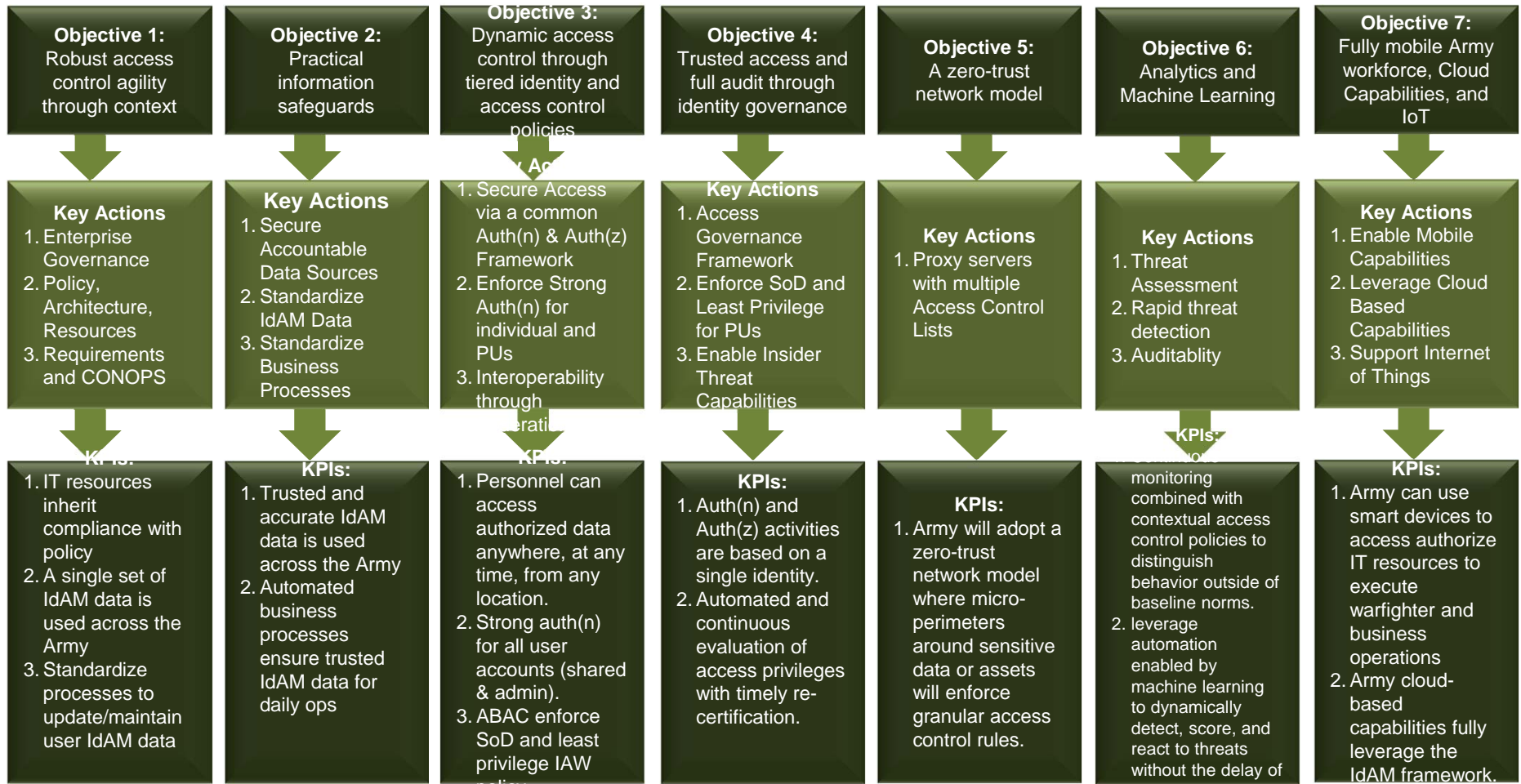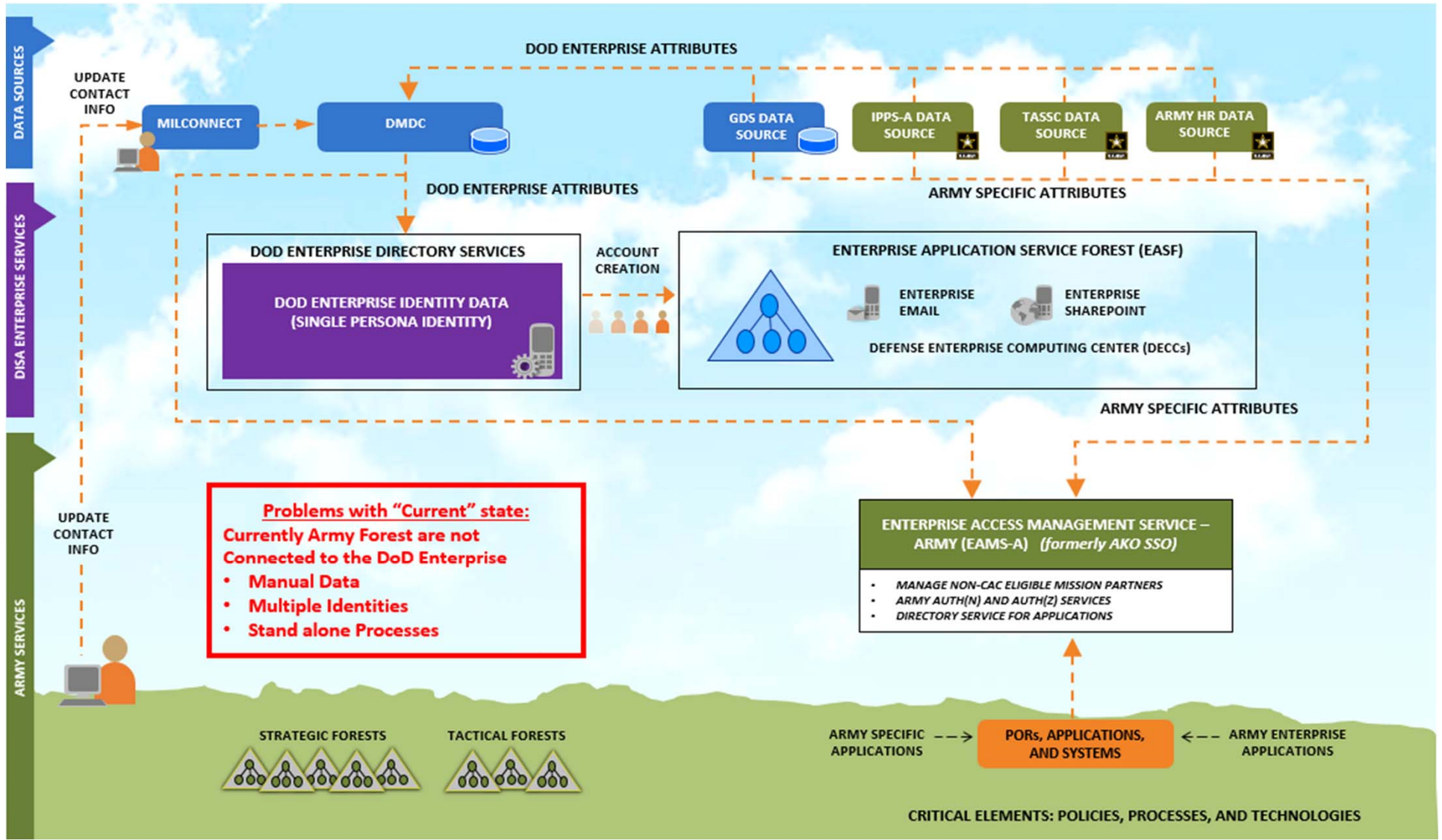
SOLDIERS • FAMILIES • ARMY CIVILIANS
ARMY STRONG.

Army IdAM Concept: Core Information

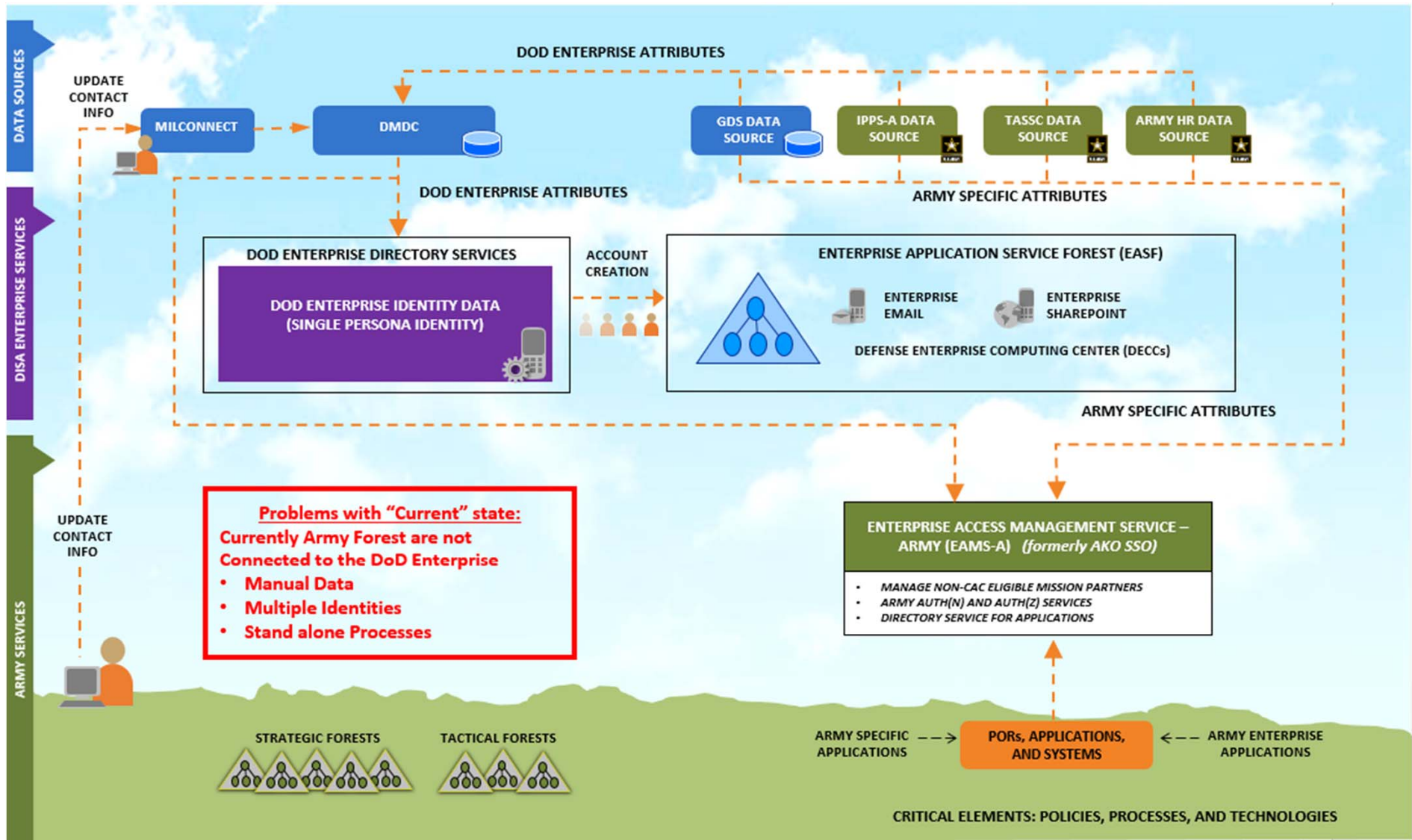## The Army Objectives, Key Actions, and Key Performance Indicators

Objective 1: Robust access control agility through context	Objective 2: Practical information safeguards	Objective 3: Dynamic access control through tiered identity and access control policies	Objective 4: Trusted access and full audit through identity governance	Objective 5: A zero-trust network model	Objective 6: Analytics and Machine Learning	Objective 7: Fully mobile Army workforce, Cloud Capabilities, and IoT
Key Actions 1. Enterprise Governance 2. Policy, Architecture, Resources 3. Requirements and CONOPS	**Key Actions** 1. Secure Accountable Data Sources 2. Standardize IdAM Data 3. Standardize Business Processes	**Key Actions** 1. Secure Access via a common Auth(n) & Auth(z) Framework 2. Enforce Strong Auth(n) for individual and PUs 3. Interoperability through ...eration	**Key Actions** 1. Access Governance Framework 2. Enforce SoD and Least Privilege for PUs 3. Enable Insider Threat Capabilities	**Key Actions** 1. Proxy servers with multiple Access Control Lists	**Key Actions** 1. Threat Assessment 2. Rapid threat detection 3. Auditablity	**Key Actions** 1. Enable Mobile Capabilities 2. Leverage Cloud Based Capabilities 3. Support Internet of Things
KPIs: 1. IT resources inherit compliance with policy 2. A single set of IdAM data is used across the Army 3. Standardize processes to update/maintain user IdAM data	**KPIs:** 1. Trusted and accurate IdAM data is used across the Army 2. Automated business processes ensure trusted IdAM data for daily ops	**KPIs:** 1. Personnel can access authorized data anywhere, at any time, from any location. 2. Strong auth(n) for all user accounts (shared & admin). 3. ABAC enforce SoD and least privilege IAW ...licy	**KPIs:** 1. Auth(n) and Auth(z) activities are based on a single identity. 2. Automated and continuous evaluation of access privileges with timely re-certification.	**KPIs:** 1. Army will adopt a zero-trust network model where micro-perimeters around sensitive data or assets will enforce granular access control rules.	**KPIs:** ...continuous monitoring combined with contextual access control policies to distinguish behavior outside of baseline norms. 2. leverage automation enabled by machine learning to dynamically detect, score, and react to threats without the delay of ... intervention	**KPIs:** 1. Army can use smart devices to access authorize IT resources to execute warfighter and business operations 2. Army cloud-based capabilities fully leverage the IdAM framework.

Current State Enterprise IdAM Business Process Architecture

DATA SOURCES

DOD ENTERPRISE ATTRIBUTES

UPDATE CONTACT INFO

MILCONNECT → DMDC

GDS DATA SOURCE | IPPS-A DATA SOURCE | TASSC DATA SOURCE | ARMY HR DATA SOURCE

DISA ENTERPRISE SERVICES

DOD ENTERPRISE ATTRIBUTES

ARMY SPECIFIC ATTRIBUTES

DOD ENTERPRISE DIRECTORY SERVICES

DOD ENTERPRISE IDENTITY DATA (SINGLE PERSONA IDENTITY)

ACCOUNT CREATION

ENTERPRISE APPLICATION SERVICE FOREST (EASF)

ENTERPRISE EMAIL | ENTERPRISE SHAREPOINT

DEFENSE ENTERPRISE COMPUTING CENTER (DECCs)

ARMY SPECIFIC ATTRIBUTES

ARMY SERVICES

UPDATE CONTACT INFO

Problems with "Current" state:
Currently Army Forest are not Connected to the DoD Enterprise
- **Manual Data**
- **Multiple Identities**
- **Stand alone Processes**

ENTERPRISE ACCESS MANAGEMENT SERVICE – ARMY (EAMS-A) *(formerly AKO SSO)*

- MANAGE NON-CAC ELIGIBLE MISSION PARTNERS
- ARMY AUTH(N) AND AUTH(Z) SERVICES
- DIRECTORY SERVICE FOR APPLICATIONS

STRATEGIC FORESTS | TACTICAL FORESTS

ARMY SPECIFIC APPLICATIONS → PORs, APPLICATIONS, AND SYSTEMS ← ARMY ENTERPRISE APPLICATIONS

CRITICAL ELEMENTS: POLICIES, PROCESSES, AND TECHNOLOGIES

SOLDIERS • FAMILIES • ARMY CIVILIANS
ARMY STRONG.

Future State Enterprise IdAM
Business Process Architecture

Army IdAM: What is Next Step?

Establish a Synchronized Approach to Reach the Desired End State

Develop Courses of Action achieve the Army IdAM Vision Objectives:

Objective 1:
Robust Access Control

Objective 2:
Practical Information Safeguards

Objective 3:
Dynamic Access Control through policies

Objective 4:
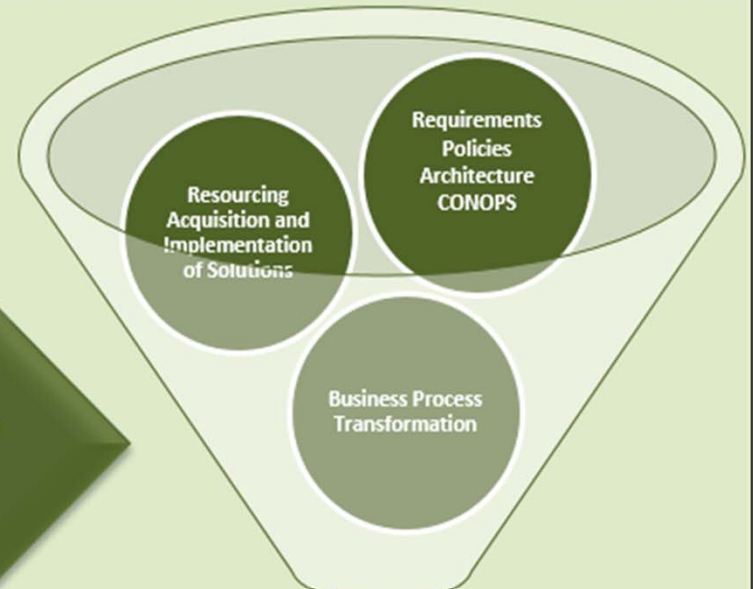Trusted Access/Auditing and Governance

Objective 5:
Zero-trust network model

Objective 6:
Analytics and machine learning

Objective 7:
Fully mobile Army workforce, Cloud Capabilities, and IoT

Determine and Align What Stakeholders Need

- Resourcing Acquisition and Implementation of Solutions
- Requirements Policies Architecture CONOPS
- Business Process Transformation

Army On/Off Premises IdAM Solution

SOLDIERS • FAMILIES • ARMY CIVILIANS
ARMY STRONG.

Significance of IdAM Capability
Federal, DoD, and Army Guidance

DoD IdAM Strategy Objectives

- Access Control is Dynamic
- DoD IdAM Data is Complete, Trusted, Accurate and Accessible
- Access Accountability is Enhanced
- Entity Contact Data can be Discovered
- Collaboration and Interoperability are Enhanced
- DoD IdAM Institutionalized

DoD CIO EDS Mandate

- Use Enterprise Directory Services to populate /maintain authoritative org and contact data in DMDC
- *Populate and sync directories* (i.e. applications, systems, etc.) with *enterprise data (Single Identity)*
- Use Enterprise Directory Services in future procurements, contracts, and technical designs

DoD Memo: Insider Threat

- Define and *enforce limits on overt access*
- Accountability for actions through reliable (non-refutable) records
- *Detection of unauthorized activity*
- *Mitigation of unauthorized activity*
- Response to unauthorized activity

Army Network Campaign Plan

- **Vision:** A *secure, integrated, standards-based environment that ensures* uninterrupted *global access and enables collaboration* and decisive action *throughout all operational phases across all environments*
- **Mission Statement:** The CIO/G-6 Leads Army network modernization to *deliver timely, trusted, and shared information* for the Army and it's mission partners.

America's Force of Decisive Action   For Official Use Only   8

SOLDIERS • FAMILIES • ARMY CIVILIANS
ARMY STRONG.