



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DEFENSE ENTERPRISE IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT (ICAM)

July 2020

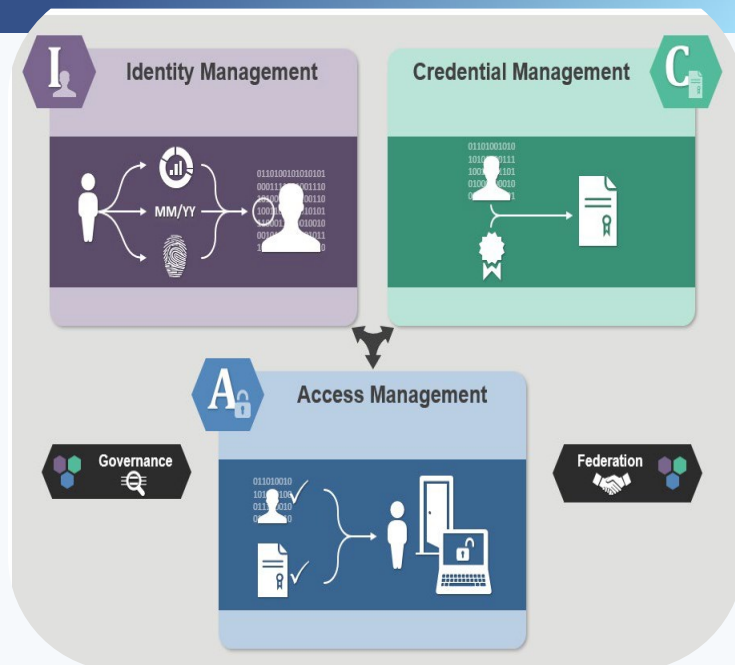
Defense Enterprise ICAM Vision: To provide a secure and trusted environment where people and systems can securely access all authorized resources based on mission need

Defense Enterprise ICAM Approach:

- DoD components will publish information directly from their existing data silos and then share this data across the enterprise using commercial tools
- This will create logical views or translation layers that work with existing component and enterprise identity and attribute services, enabling shared enterprise capabilities

Key Capabilities:

- Centralized and federated authentication services that ensure alternative multifactor authentication above and beyond the Common Access Card via an Identity Provider (IDP)
- Identity governance and account lifecycle management to automate account provisioning/de-provisioning to ensure reporting and access attestation/recertification via the Automated Account Provisioning (AAP)
- Enterprise aggregation, analytics, and audit of access and roles, and implementing segregation of duty rules across applications and DoD organizations via the Master User Record (MUR)



Defense Enterprise ICAM Enhancements for FY20 and Beyond

- Enable new computing form factors and platforms
- Utilize continuous multifactor authentication
- Centralize identity provider for authentication
- Enable attribute and data sharing among DoD organizations
- Automate account creation and deletion
- Enable a zero trust architecture
- Enable system behavioral pattern indicators