DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DoD Enterprise Identity, Credential and Access Management (ICAM)

Chandler Grice
Brandon Iske
Cyber Security and Analytics Directorate
April 2022

DISCLAIMER

The information provided in this briefing is provided for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

DoD is Modernizing Identity

Username/Password

- Poor Security

DEERS RAPIDS + DoD CAC/PIV

- High Security
- Strong Identity Vetting
- Smart Card
- Complex

DoD Derived Credentials

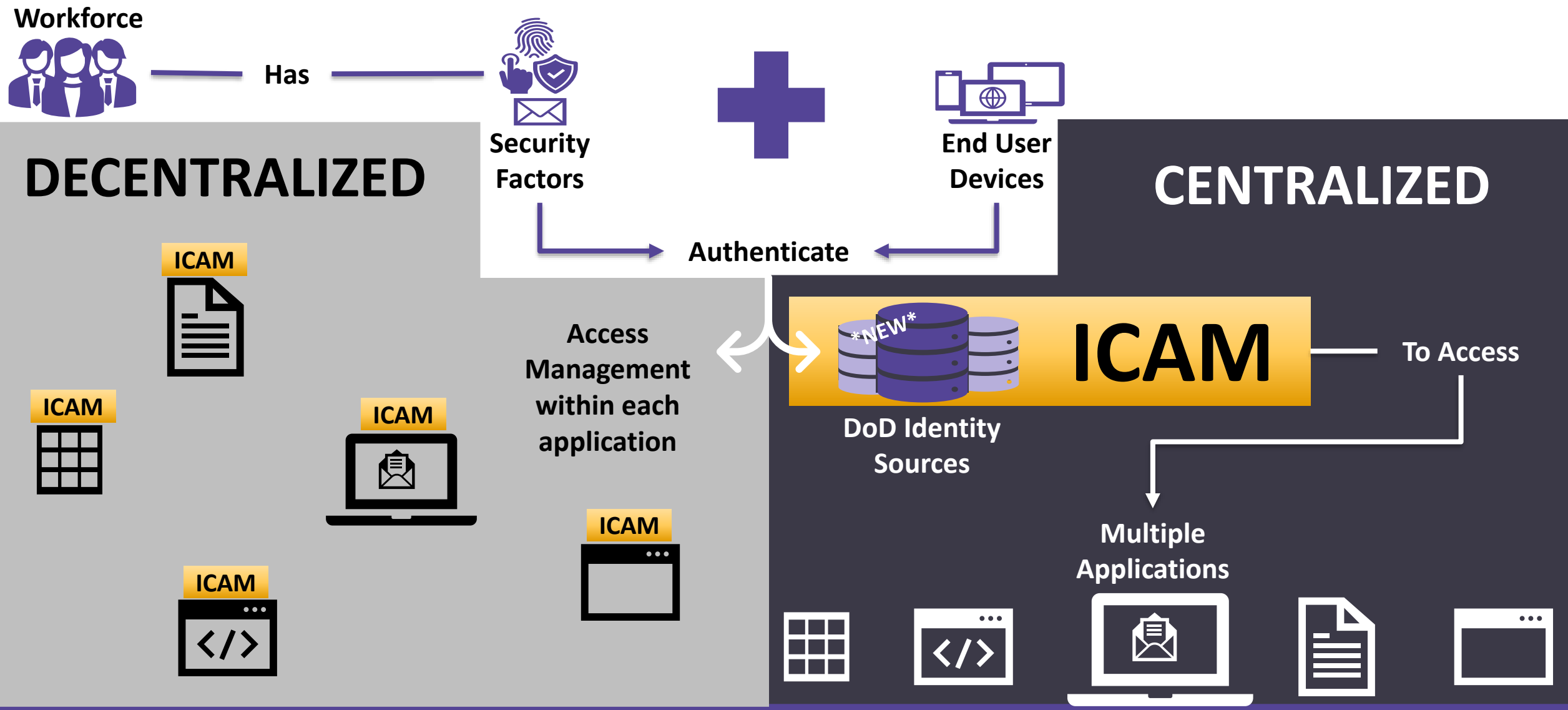
- High Security
- Mobile
- Interoperable

2022+ DoD ICAM Access Management

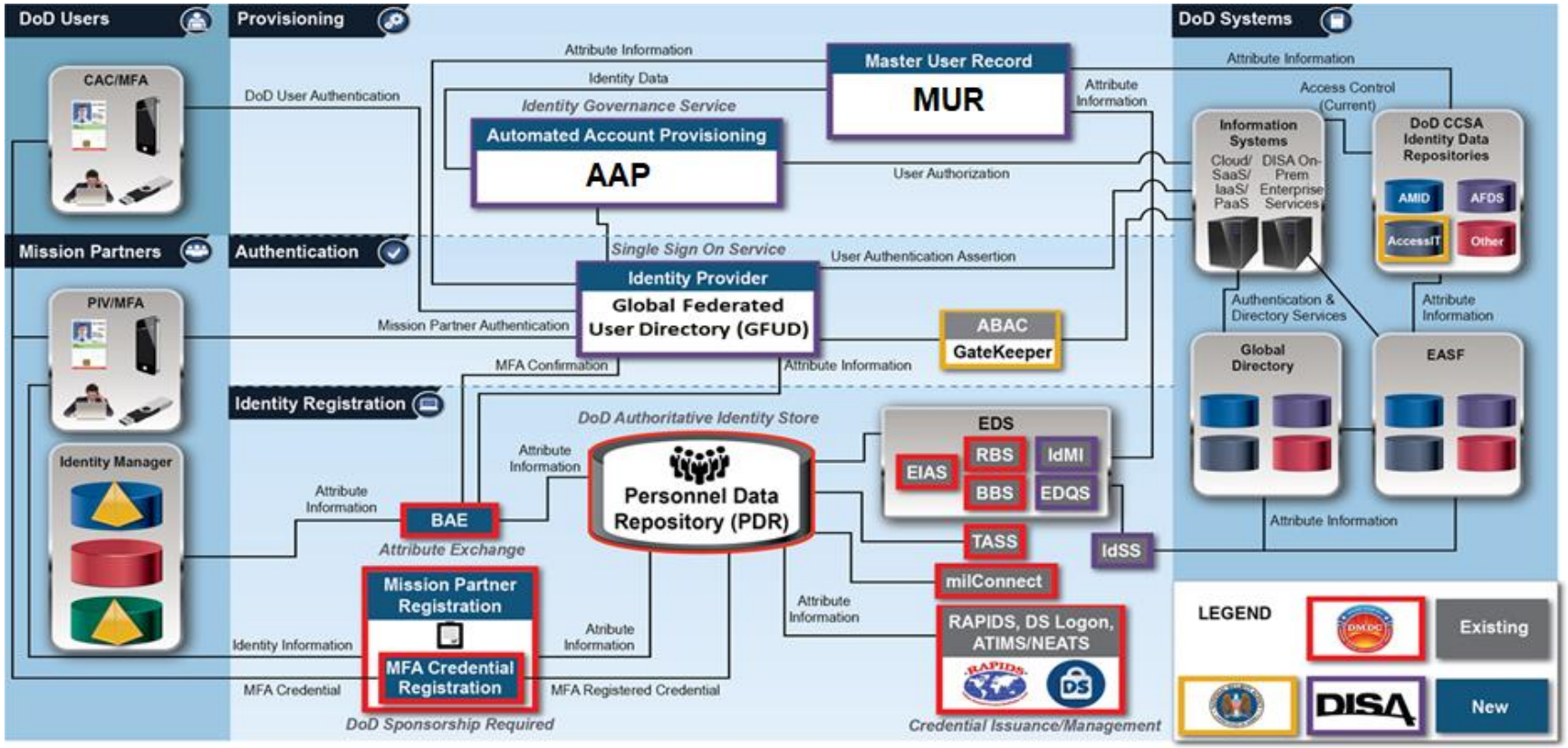
- Account Automation
- Centralized & Continuous Authentication
- Data and Attribute Sharing
- New Platforms and MFA

Zero Trust

Centralized Integration Enables Zero Trust and Scalability



Components of Enterprise ICAM



Identify Provider (IDP): Centralizes authentication and enables alternative multifactor authentication beyond DoD CAC holders

Automated Account Provisioning (AAP): Enables workflows, self service, and automation to improve data access

Master User Record (MUR): Aggregates application account data at the enterprise-level to audit who has access to what across DoD organizations

ICAM Federation

Why Federate? Federation enables one organization to accept another organization's work. Federation is based on inter-organizational trust.

Who is Federating?

- ❑ Federation between DoD enterprise and DoD Component ICAM services
- ❑ Federation with external mission partners
  - Federal government
  - Allied and coalition partners
  - State, local, territorial, tribal government
  - Defense Industrial Base (DIB)
  - Non-governmental organizations
  - Commercial providers of beneficiary services
- ❑ Federation between cloud tenants

What is being Federated?

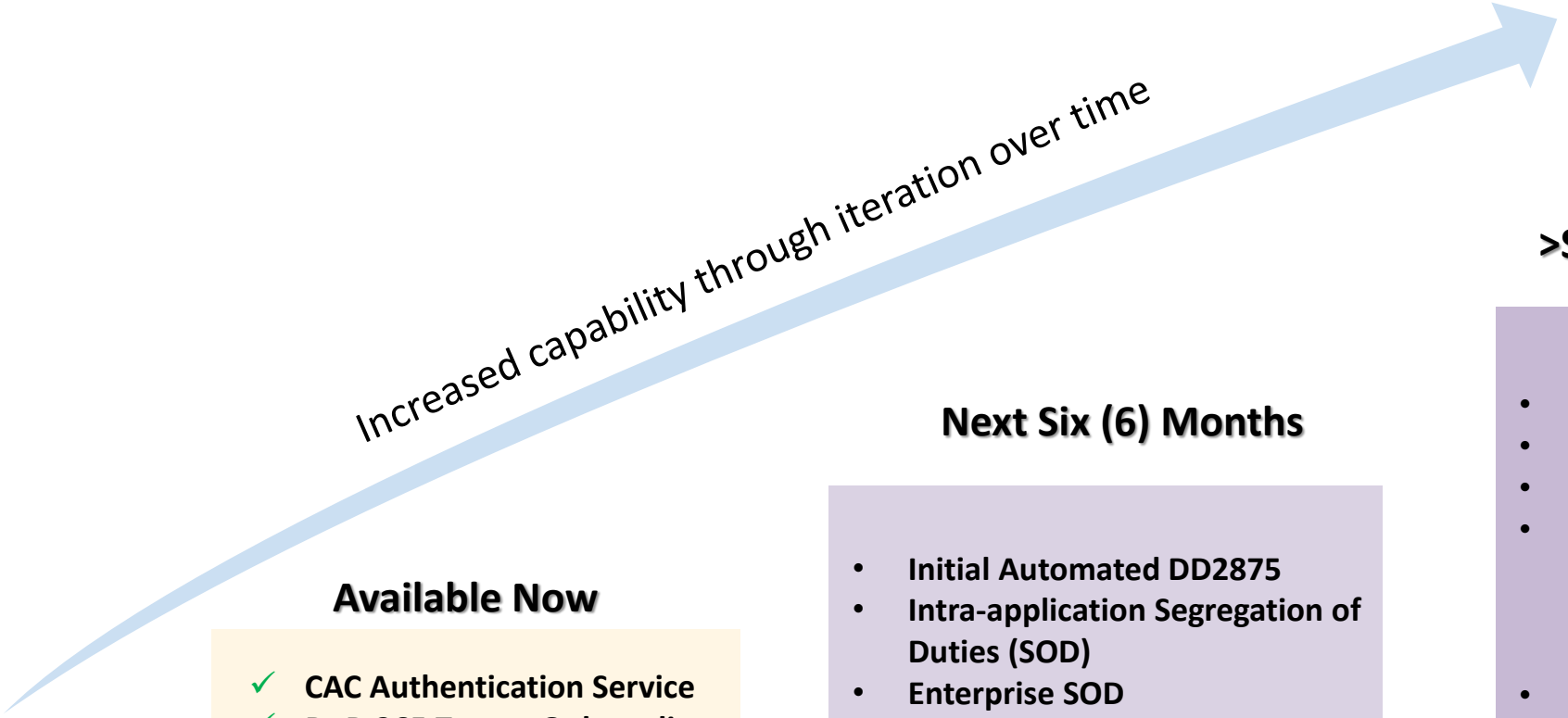
- Onboarding
- Identity
- Credentials
- Provisioning
- Authentication
- Authorization

Next Steps:

1) Define criteria for adopting DoD Enterprise ICAM vs DoD Component ICAM solution

2) Leverage lessons learned from EDU/Internet2 for DoD/Fed Gov't federation planning

Foundational ICAM Capabilities & Roadmap



Available Now

- ✓ CAC Authentication Service
- ✓ DoD 365 Tenant Onboarding
- ✓ Multi-Factor Authentication (MFA) for CAC-holders
- ✓ Self-Service Portal
- ✓ CAC Identity Feeds

Next Six (6) Months

- Initial Automated DD2875
- Intra-application Segregation of Duties (SOD)
- Enterprise SOD
- Initial SIPR capability
- Self-Service Portal expansion
- Continual enhancements
- Federation criteria and priorities

>Six (6) Months (Evolving)

- MFA Expansion
- Federated Identity
- Federated Provisioning
- Federated Authentication
  - DoD IdP to DoD IDP
  - DoD IdP to Fed
  - DoD IdP to Coalition
- SIPR Expansion
- DoD Licensing Strategy
- Denied, degraded, intermittent, limited solutions
- Privileged Access Management (PAM)

How To Engage & Onboard

- **GFUD Authentication/Directory Services:**
  - **The Mission Partner Web application:**
    - Must be able to use the attributes provided as apart of GFUD existing claim configuration
    - Must be capable of accepting claims (claims-aware)
    - Must be able to communicate with the GFUD service endpoint over SSL (port 443)
    - Applicable DoD and commercial certificates must be installed and trusted by the application and the user endpoint

  - **Information:**
    - Website: www.deas.mil; cyber.mil/idam
    - User Self Service Portal: https://portal.apps.deas.mil/
    - Endpoint URL: https://sts1.auth.ecuf.deas.mil/
      Metadata URL for NIPR: https://sts1.auth.ecuf.deas.mil/federationmetadata/2007-06/federationmetadata.xml
    - POC: disa.meade.sel.list.sel62-dee-ad@mail.mil
    - CC: disa.meade.se.mbx.idss-connections@mail.mil

- **Automated Account Provisioning / Master User record:**
  - DoD365 Teams site
  - Review 101 overview brief, FAQs, API guide
  - POC: disaicam@mail.mil

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

/DISA **@USDISA** **/USDISA** **DISA.mil**