



# Product Leader Enterprise Content Collaboration and Messaging (PL EC2M) AFCEA Belvoir Industry Day

**Connecting the Army.  
Working for Soldiers.**

**Nov. 4, 2021**





U.S. ARMY



# BREAK OUT SESSION

## AFCEA Belvoir Industry Day

Identity Credential and Access Management (ICAM)



**Mr. Steve Vonderheide**  
Project Officer  
ICAM



**Mr. David Thompson**  
Acting Product Lead  
EC2M





# ICAM Program Overview



- **Background:** Historically, Army organizations worked independently to develop, procure, and implement IT resources for mission requirements. This resulted in the following major issues and challenges:
  - Multiple identities that hinder info sharing and collaboration (e.g. O365, [cvr@mail.mil](mailto:cvr@mail.mil), AKO user name, DEE user name).
  - Inability to uniquely identify, authenticate, and audit user network transactions across different security boundaries.
  - Procurement of redundant systems, services, manpower, and hardware.
  - No common standard which contributes to complex, disparate networks, & stove-piped systems that lack interoperability.
- **Key Stakeholder Activities:** The Army ICAM IPT assessed and developed the following artifacts to resolve capability gaps
  - Army ICAM Strategy & Roadmap, 15 JUL 2020
  - Army ICAM and PKI Pamphlet 25-2-13, 04 APR 2019 (under update)
  - Army Identity Attribute Specification, 23 SEP 2019
  - Army ICAM Requirements Definition Package, (In Progress)
  - Army ICAM Functional Requirements (Stop Gap)
  - Army ICAM CONOPs (In Progress)
- ICAM IPT members: CIO, G-6, CCoE, ARCYBER, PEO EIS, PEO C3T, PEO Soldier, NETCOM, and C5ISR Center.
- **End State:** A global, robust ICAM capability that leverages a single set of authoritative identity data to grant access to authorized IT resources at the point of need regardless of location.
  - Entire DoD CAC and Army non CAC eligible mission partners (i.e. First responders, non contract cadets, IRR, Academia, etc.)
  - Alternative Multifactor Authentication (includes Soldiers without GFE)
  - Cloud autonomous ICAM capabilities outside the DoDIN
  - Risk-based decision on GFE and non GFE access
- **Objective:** Maintain baseline ICAM requirements while adopting Zero Trust capabilities inside and outside of the DoDIN using scalable and interoperable technologies.
- **Army Branded ICAM Capabilities:** Army Master Identity Directory (AMID) and Enterprise Access Management Service – Army (EAMS-A) are “capabilities” not technical solutions. The objective is to:
  - Remain completely vendor agnostic with plug and play capability
  - Place the onus on vendors to allocate resources to remain interoperable with current Army solutions
  - Ensure capabilities are fully funded, compliant with policy, and provide inheritable RMF security controls to IT systems
  - Leverage the existing Army Enterprise Service Desk Worldwide (AESD-W) support already provided for EAMS-A to prevent redundant cost.
  - Provide the same ICAM capabilities for Army IT resources that have a non CAC eligible user population in the cloud.



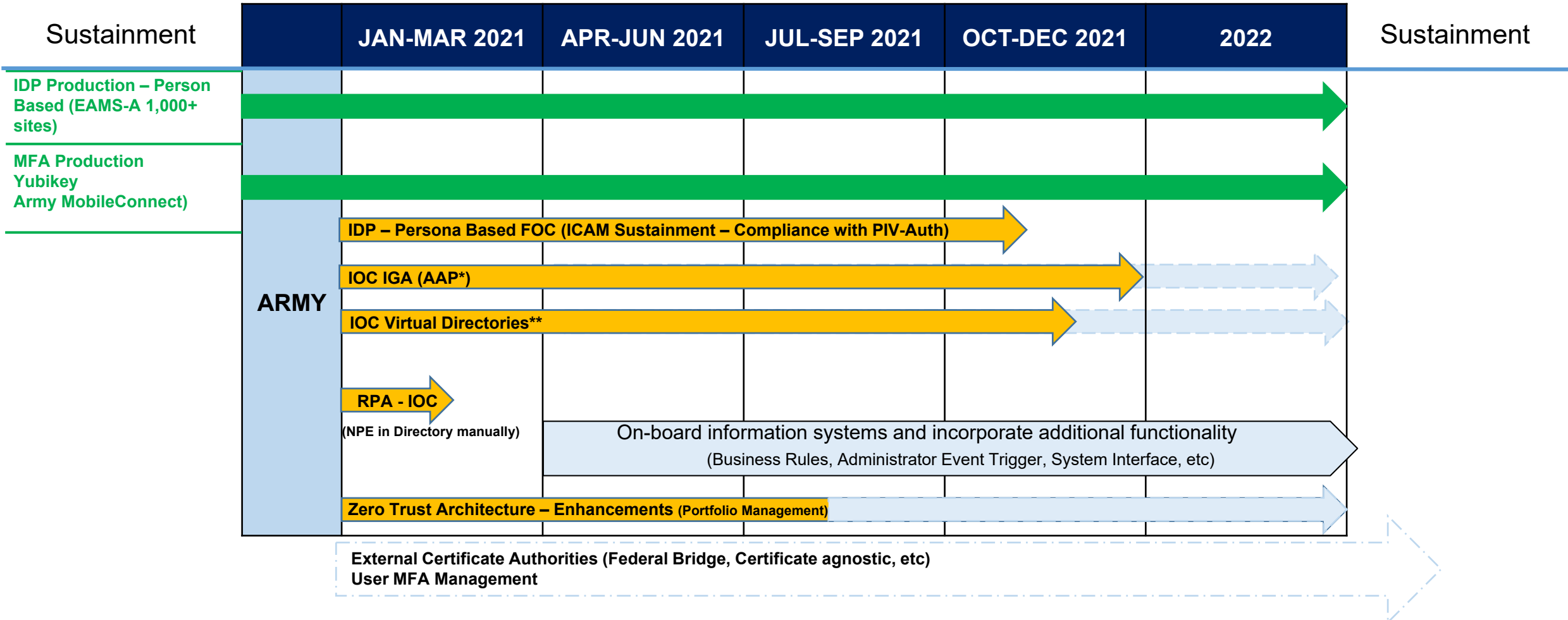
# ICAM Activity: Phase 1



ICAM Functions	Capabilities	ICAM Functions	Capabilities
Identity Management	<p>ICAM Portal (AMID)</p> <ul style="list-style-type: none"> <li>- Onboarding &amp; Registration</li> <li>- Sponsorship (Army non-CAC)</li> <li>- Provisioning &amp; Entitlement Management</li> <li>- Access Review &amp; Recertification (Audit)</li> </ul>	Credential Management	<p>DMDC</p> <ul style="list-style-type: none"> <li>- CAC Issuance</li> <li>- Enterprise Username</li> <li>- Robotic Process Automation (RPA)</li> </ul> <p>Manual input for testing - IOC</p>
Identity Governance and Administration	<p>IGA</p> <ul style="list-style-type: none"> <li>- Audit and Reporting</li> <li>- Separation of Duties</li> </ul>	Directory Services	<p>AMID</p> <ul style="list-style-type: none"> <li>- Custom Views</li> <li>- Identity record synchronization</li> <li>- Attributes, Identities</li> </ul>
Access Management	<p>EAMS-A</p> <ul style="list-style-type: none"> <li>- Authentication (MFA: CAC, Yubikey, MobileConnect)</li> <li>- Authorization (Cookie: Policy stores)</li> <li>- ABAC</li> </ul> <p>Boundary Control</p> <ul style="list-style-type: none"> <li>- Zero Trust Architecture (ZTA)</li> </ul> <p>Increasing compliance with ZTA</p>	Federation	<p>External Certificate Authorities</p> <p>Non-DoD credentials</p>



# ICAM Roadmap: Phase 1



- Notes:
- \*AAP – Automated Account Provisioning IOC is automating the 2875 (Notification to system administrators): FOC Interface with system implemented
  - \*\* IOC Virtual Directories IOC – Synchronize with 22 AD Domains: FOC
  - \*\*\* SIPR also in production



# ICAM Activity: Phase 2



ICAM Functions	Capabilities	ICAM Functions	Capabilities
Identity Management	<p>ICAM Portal (AMID)</p> <ul style="list-style-type: none"> <li>- Onboarding &amp; Registration</li> <li>- Sponsorship (Army non-CAC)</li> <li>- Provisioning &amp;Entitlement Management</li> <li>- Access Review &amp; Recertification (Audit)</li> <li>- Identity Proofing</li> <li>- NPE Identities (Devices vs RPAs)</li> </ul>	Credential Management	<p>DMDC</p> <ul style="list-style-type: none"> <li>- CAC Issuance</li> <li>- Enterprise Username</li> <li>- Non-person Entity Credentials</li> <li>- Robotic Process Automation (RPA) <ul style="list-style-type: none"> <li>- Person vs non-person</li> </ul> </li> </ul>
Identity Governance and Administration	<p>IGA</p> <ul style="list-style-type: none"> <li>- Audit and Reporting</li> <li>- Context Awareness</li> <li>- Separation of Duties</li> <li>- Risk Management/Profiling</li> </ul>	Directory Services	<p>AMID</p> <ul style="list-style-type: none"> <li>- Custom Views</li> <li>- Identity record synchronization</li> <li>- Attributes, Identities</li> <li>- NPE Attributes</li> </ul>
Access Management	<p>EAMS-A</p> <ul style="list-style-type: none"> <li>- Authentication (MFA: CAC, Yubikey, MobileConnect))</li> <li>- Authorization (Cookie: Policy stores)</li> <li>- ABAC</li> <li>- Privileged User</li> </ul> <p>Boundary Control</p> <ul style="list-style-type: none"> <li>- Zero Trust Architecture</li> <li>- Session Management</li> </ul>	Federation	<p>External Certificate Authorities</p> <ul style="list-style-type: none"> <li>- Approval Process</li> <li>- OCSP-like capability (No crls)</li> </ul> <p>Non-DoD credentials</p>



# ICAM Roadmap: Phase 2



Sustainment

JAN-MAR 2021

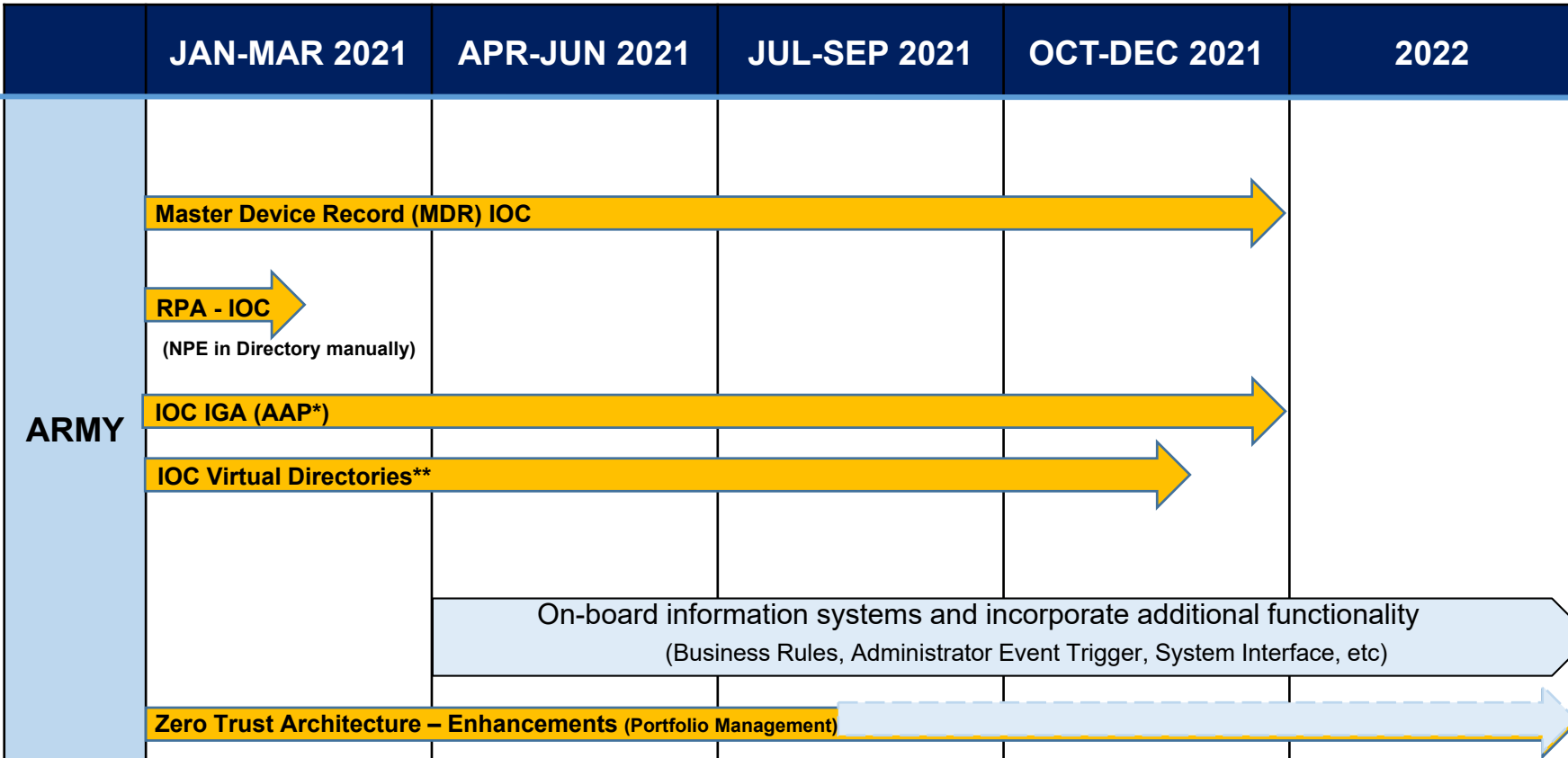
APR-JUN 2021

JUL-SEP 2021

OCT-DEC 2021

2022

Sustainment

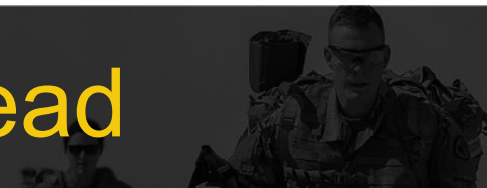


External Certificate Authorities (Federal Bridge, Certificate agnostic, etc)  
 User MFA Management

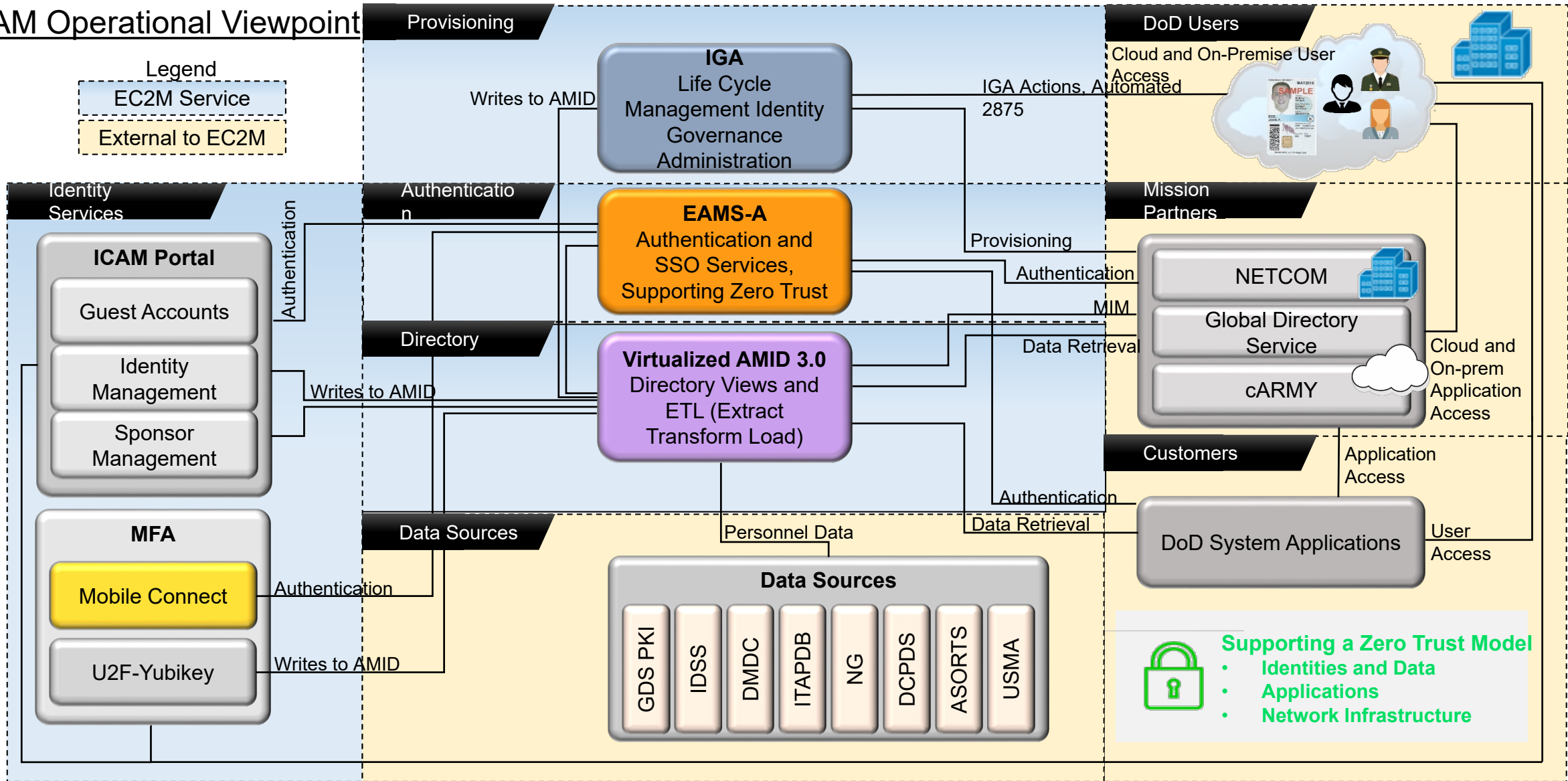
- Notes:
- \*AAP – Automated Account Provisioning IOC is automating the 2875 (Notification to system administrators): FOC Interface with system implemented
  - \*\* IOC Virtual Directories IOC – Synchronize with 22 AD Domains: FOC
  - \*\*\* SIPR also in production



# ICAM Way Ahead



## ICAM Operational Viewpoint







# Closing



## **The 4 pillars of the Army ICAM platform are:**

1. Identity Directory Services – Virtualized AMID
2. Authentication and Network Authorization – EAMS-A
3. Identity and Governance Administration - IGA  
– Access and Account Lifecycle Management
4. Credential Issuance and Lifecycle Management\* – PKI

\* The fourth pillar is integrated with the Army ICAM platform, but managed separately

## **Existing Capabilities**

- Authentication/Authorization, validating user identity and permissions
- Identity store, attributes for identity records
- MFA: CAC/Yubikey/Army Mobile Connect

## **Future Capabilities**

- Identity Governance and Administration (IGA): Automated Account Provisioning (AAP) and Automated 2875
- Virtualized Directories: Custom AMID views
- Provide a secure environment with compliance to NIST 800-63 Rev 3 for Zero Trust security model
- IPPS-A integration as a new authoritative data source


## **Objective:**


Maintain baseline ICAM requirements while adopting Zero Trust capabilities inside and outside of the DoDIN using scalable and interoperable technologies.




# Questions

**Connecting the Army.**  
**Working for Soldiers.**

 [Company/usarmypeoeis](https://www.linkedin.com/company/usarmypeoeis)

 [peo.eis](https://www.facebook.com/peo.eis)

 [@PEOEISPAOffice](https://twitter.com/PEOEISPAOffice)

 [www.eis.army.mil](http://www.eis.army.mil)

