

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

**AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA**

Identity, Credential, and Access Management (ICAM): The Keystone for Mission-Ready Care and Command *Identity as the New Perimeter*

Mr. Joshua Zamarripa, E-MBA, CISSP, S+, ITIL

Mr. Bryan Scott, CISSP

UNCLASSIFIED



Agenda

1

The Operational Pain: Fragmented Access

The Status Quo: The clinical, security, and administrative costs of legacy login fatigue and fragmented access.

2

Establishing the ICAM Keystone

The Solution: What ICAM is, why it is mandated, and the enterprise tools driving it.

3

MTF Operational Impact

The Operational Value: Reclaiming clinical minutes, protecting patient data, and transitioning from "Trust but Verify" to "Never Trust".

4

DHA ICAM Application Onboarding

The Rules of Engagement: Evaluating application prerequisites, leveraging the self-service portal, and aligning local systems with enterprise mandates.

5

Call to Action & Resources

The Marching Orders: Moving from supervisors to Data Owners, automating 2875s (SAARs), and utilizing DHA onboarding resources.

Speaker Introduction



Mr. Joshua Zamarripa
E-MBA, CISSP, S+, ITIL

Infrastructure &
Operations Division
Defense Health Agency



Mr. Bryan Scott
CISSP

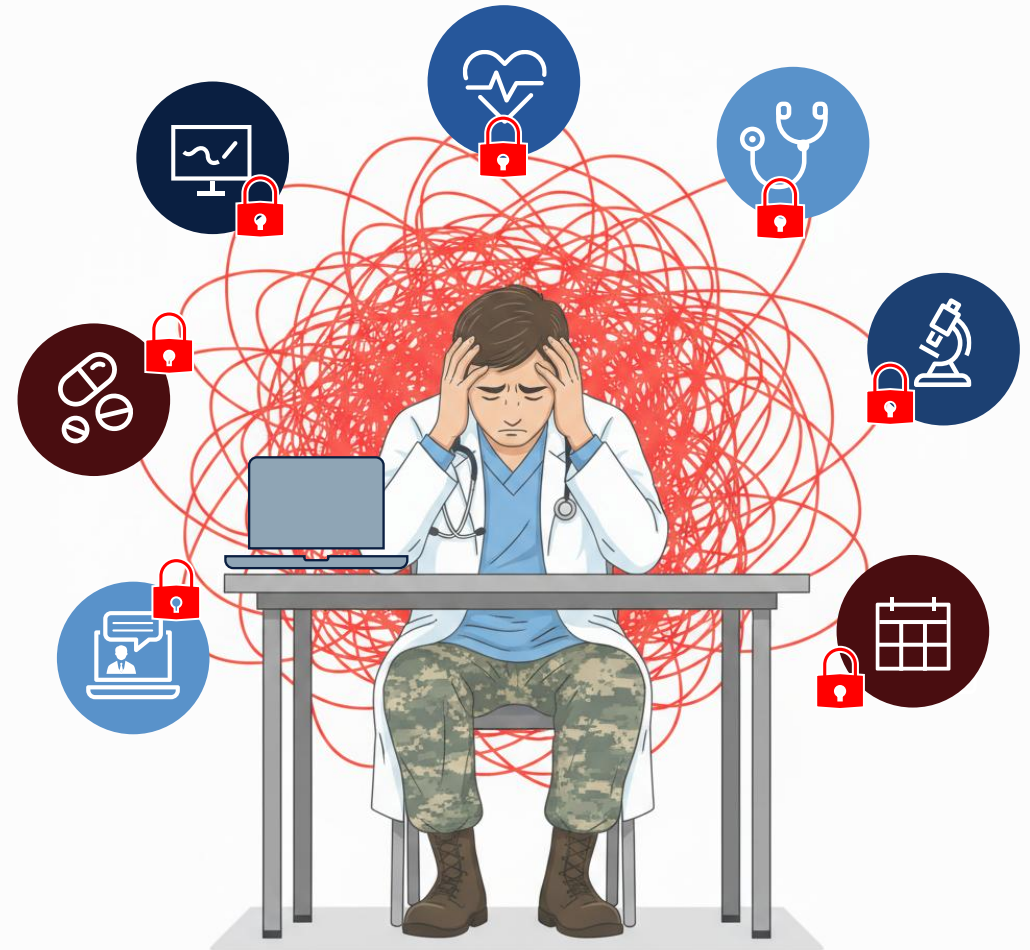
Infrastructure &
Operations Division
Defense Health Agency

Learning Objectives

- 1** Explain the role of ICAM as the foundation of Zero Trust and enterprise security.
- 2** Describe how identity verification enables secure access to healthcare systems.
- 3** Identify how ICAM supports mission operations by enabling the right access for the right person at the right time.
- 4** Recognize the connection between identity management and operational readiness.

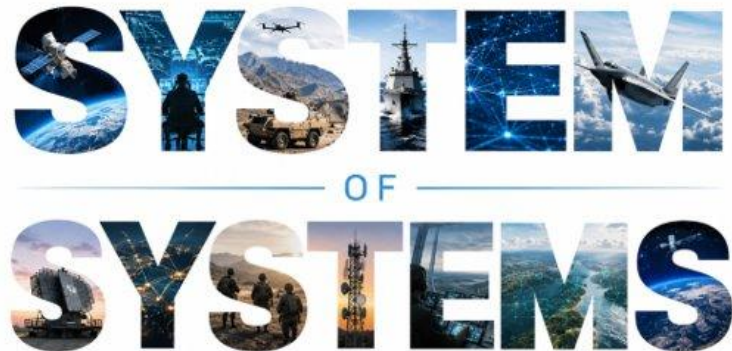
The Operational Pain: Fragmented Access

- Delayed Patient Care
 - Administrative friction at the terminal slows down critical clinical workflows.
- Frustrated Staff Workarounds
 - Siloed logins lead to dangerous shortcuts, such as the chronic issue of left-behind CACs in shared workstations.
- Administrative Overload
 - Disconnected systems generate massive, unsustainable helpdesk password reset volumes, draining IT resources.
- Increased Cyber Risk
 - Fragmented authentication expands the attack surface, leaving sensitive data vulnerable to lateral movement.



Identity, Credential, and Access Management (ICAM)

ICAM is a framework of policies, processes, and technologies used to manage digital identities, grant access to resources, and ensure that only authorized users can access sensitive information and systems. It's a critical component of cybersecurity and data protection.



- We can't 'procure' an 'off-the-shelf' ICAM due to its complexity and the need for customization
- ICAM is mandated for **all** applications and services by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and Department of War (DoW)
- The DHA is implementing ICAM incrementally and iteratively
- ICAM is a foundational component of Zero Trust

Establishing the Keystone: Identity-Centric Security

ICAM continuously answers three critical questions:

1. **Identity:** Who are you?
Verifying the user
2. **Credential:** Can you prove it?
Strong, integrated MFA
3. **Access:** What are you authorized to see?
Enforcing least-privilege permissions



Components of DHA's Mission Specific ICAM



Identity Provider (IdP)

Ping Identity Suite

- Provides authentication services
- Builds rules and policies to enforce access control



Identity Governance & Administration (IGA)

SailPoint

- Manages identity lifecycle, automation, audit and compliance



Master Entitlement Record (MER)

Radiant Logic

- Contains information about identities (users, devices, applications) and their attributes

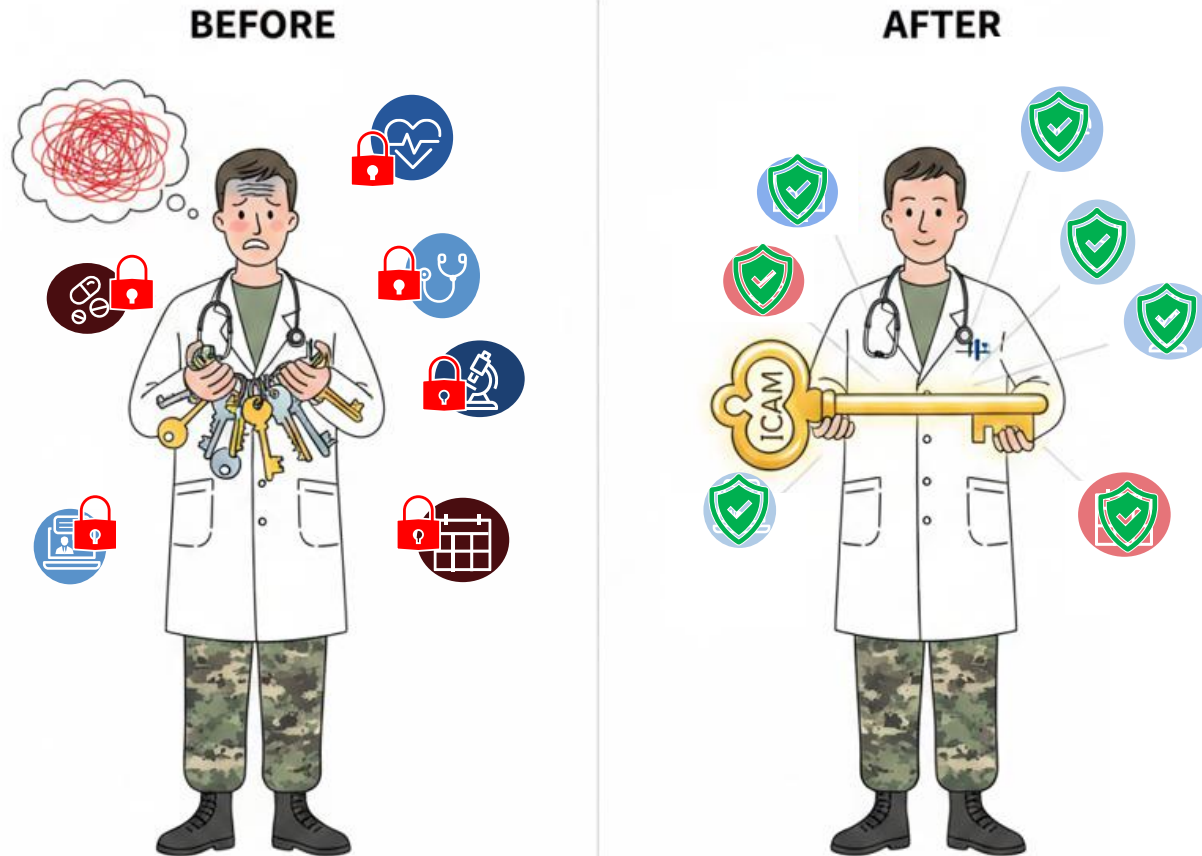


Privileged Identity Management (PIM) / Privileged Access Management (PAM)

Beyond Trust

- Controls administrative privileges

Transforming the Provider Experience



At its core, ICAM is the enterprise "master key". It shifts security away from the network perimeter directly to the user and the data.

- Elimination of "Login Fatigue"
 - Implementing enterprise Single Sign-On (SSO) removes the burden of managing multiple passwords.
- Frictionless Workflows
 - Seamless authentication allows staff to move between applications without breaking their concentration.
- Reclaiming Clinical Time
 - By removing login delays, ICAM gives clinicians back minutes per encounter to focus entirely on the warfighter, not the keyboard.

Supporting DHA Lines of Effort

- **LOE 1: Delivering Medically Ready Warfighters** - ICAM ensures clinicians and medical personnel have secure, reliable access to the systems and data required to diagnose, treat, and maintain the health readiness of warfighters.
- **LOE 2: Delivering Medical Warrior Currency** - By enabling trusted access to training platforms, operational systems, and medical data, ICAM supports the continuous readiness and proficiency of military medical personnel.

Securing the Patient Journey

- Faster Care Delivery
 - Instant, secure access to medical systems ensures care is never delayed by a locked account or system timeout.
- Secure Data Mobility
 - Records securely follow the patient across the enterprise, ensuring the right provider has the right context at the point of care.
- Uncompromised Trust
 - Zero Trust protocols ensure that highly sensitive Health Information (PHI/PII) is protected against unauthorized access or breaches.



Supporting DHA Lines of Effort

- **LOE 3: Deliver Joint Warfighting Capabilities** - ICAM establishes a trusted identity layer that allows secure collaboration and system access across military and healthcare environments, supporting joint operations and decision-making.
- **LOE 4: Deliver the Healthcare Enterprise All Beneficiaries Deserve** - By protecting sensitive data and ensuring appropriate access to healthcare systems, ICAM strengthens trust, security and efficiency in delivering care to service members, families, and beneficiaries.

From "Trust but Verify" to "Never Trust"

Feature	Legacy Environment (Perimeter-Based)	The ICAM Way (Target ZT State)
Access Model	"Trust but Verify" – Once someone is on the network (VPN/Local), they have broad lateral access or faces "siloeed" logins for every system.	"Never Trust, Always Verify" – Access is granted per-session. Users' identity, device health, and context are checked every time they touch a resource.
Authentication	Static & Fragmented. Multiple passwords for different medical databases. If one system is compromised, the attacker can move laterally.	Continuous & Integrated. Strong MFA (CAC/PIV) with backend orchestration. Identity is the common thread across all medical and tactical apps.
Provisioning	Manual/Static. Users wait days for a manual account creation in a new application. Access often remains active long after a user leaves (security risk).	Dynamic/Policy-Based. Access is tied to a user's current mission attributes. When their deployment orders end, access is revoked automatically via "Least Privilege" protocols.
Mission Impact	High Friction / High Risk. Security is a "gate" that slows down care. The "Perimeter" is easily breached and hard to defend.	Invisible Security / Resilient Mission. Security is a "guardrail" that enables care. Data is protected at the individual element level, not just the front door.

- **Frictionless Access:** Moving towards Single Sign-On (SSO) and reducing login fatigue for warfighters and staff.
- **Self-Service:** Empowering users to manage access requests without heavy helpdesk reliance.
- **Mobility & Flexibility:** Enabling secure access from various locations and approved devices.

DHA ICAM SharePoint Site

Tools & Support (i.e., Glossary & FAQs)

- FAQs can be found on the DHA-ICAM-FAQ page with category filters and a submission mechanism for ongoing updates.

Metrics & Dashboards

- The Metrics & Dashboards section contains the DHA ICAM Onboarding Dashboards.

Onboarding Process Quick Start Guide (For Application Owners)

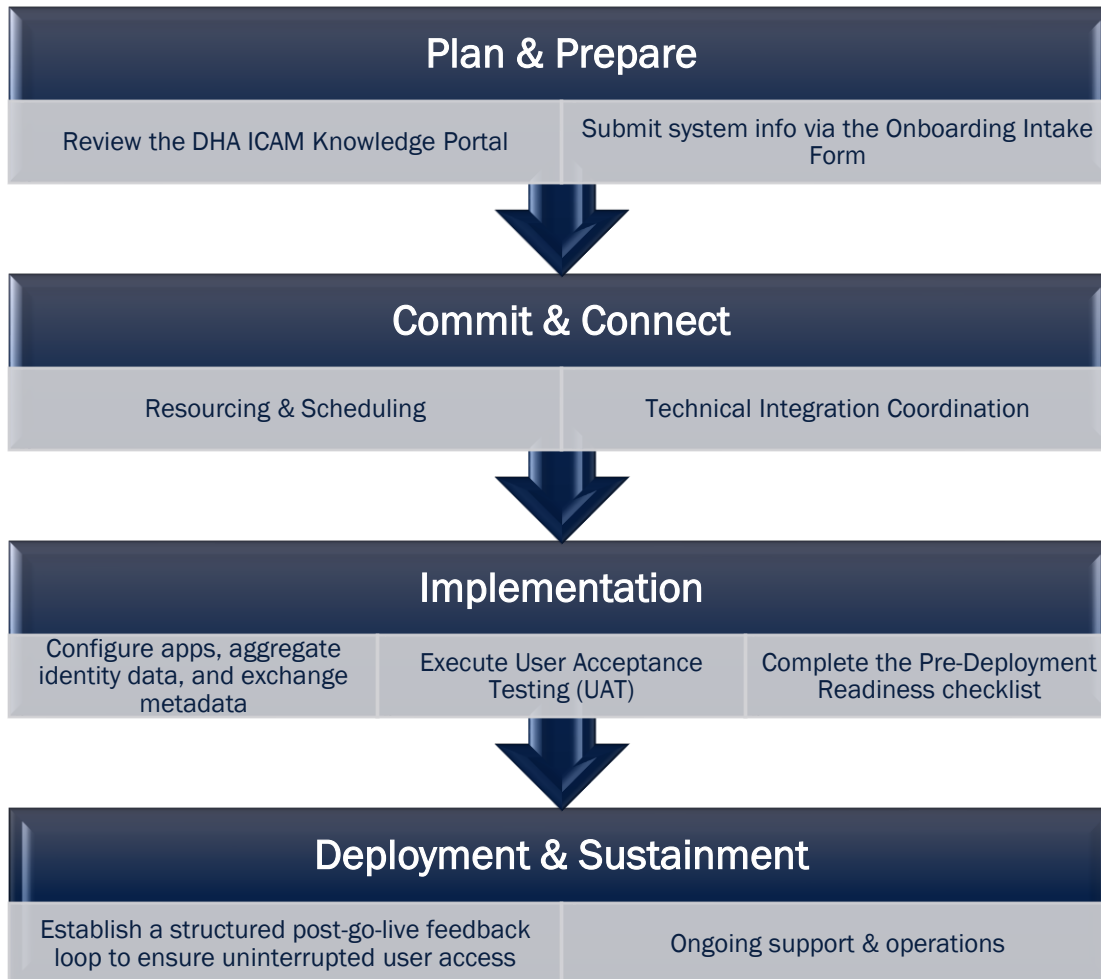
- The Quick Start Guide defines a four-phase integration methodology:
 1. Planning & Preparation
 2. Commitment & Connectivity
 3. Implementation
 4. Deployment & Sustainment

NOTE: This SharePoint site is a living resource that will continue to evolve as the ICAM program matures. Content will be regularly updated, expanded, and refined to reflect new capabilities, lessons learned, and insights gathered as the team advances implementation across DHA.



<https://militaryhealth.sharepoint-mil.us/sites/DHAICAM>

DHA ICAM Application Onboarding Checklist



Minimum Technical Requirements – Is Your App Ready?

- Active ATO: Valid Authority to Operate for at least 12 months.
- Security: Passed NIST 800-53 security assessments.
- Data Defined: Clearly defined data classification (e.g., handles PHI/PII).
- IdP Support: PingFederate/PingAccess via SAML 2.0 or OIDC/OAuth 2.0.
- MER Support: Radiant Logic via LDAP or REST API/SCIM.

(Note: SailPoint IGA and BeyondTrust PIM/PAM capabilities coming soon)



Questions?

dha.jbsa.PEO-Med-Sys-J-6.list.icam-onboarding@health.mil

Call to Action: Leading the "Identity-First" Transformation

Key Takeaway: We need your support to drive the cultural shift from legacy, manual processes to automated, identity-centric security.

The Priority: Onboarding Applications

The first step to modernization is migrating local applications to the DHA Mission-Specific ICAM service.

- Establishes the centralized foundation required for enterprise Zero Trust.

The Evolution: Unlock Automation

Partnering with ICAM unlocks critical capabilities for your facility:

- **Modernize:** Replace PDF 2875s with automated SAARs.
- **Streamline:** Automate Joiner, Mover, Leaver (JML) lifecycle.
- **Govern:** Shift approvals from Supervisors to Data Owners.
- **Prepare:** Lay groundwork for the Master Device Record.

Your Mission: Lead the Charge

As an MTF IT Leader, your immediate next steps are:

- **Champion:** Prepare hospital leadership for the transition to enterprise automation.
- **Inventory:** Identify and prioritize your local apps for integration.
- **Engage:** Leverage the ICAM SharePoint & Quick Start Guide.

DEFENSE HEALTH AGENCY



DOW APPROVED SERVICE PROVIDER

WE WANT YOU... TO GO IDENTITY-FIRST!

Join the ICAM Transformation



YOUR MISSION:

- ONBOARD APPLICATIONS, DATABASES, DEVICES
- CHAMPION NEW WORKFLOWS
- EMPOWER YOUR STAFF

THE PAYOFF:

- AUTOMATED SAARs/ NO MORE PDF 2875s
- FASTER, SECURE ACCESS
- READY FOR ZERO TRUST

Visit the DHA ICAM SharePoint Today!

DEFENSE HEALTH AGENCY



DOW APPROVED SERVICE PROVIDER

Contact

Mr. Joshua Zamarripa

DDSB Branch Chief, ICAM Program Manager

 joshua.m.zamarripa.civ@health.mil

Mr. Bryan Scott

DDSB Lead Engineer, ICAM Lead Engineer

 bryan.s.scott.civ@health.mil

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA

Thank You!



UNCLASSIFIED