DEPARTMENT OF WAR
6000 Defense Pentagon
Washington, D.C. 20301-6000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND FIELD ACTIVITY DIRECTORS

SUBJECT: Modernizing System Authorization Access Requests and Account Provisioning Through Identity, Credential, and Access Management Workflows

References: (a) DoD Instruction (DoDI) 8520.03, "Identity Authentication for Information Systems," May 19, 2023
(b) DoDI 8520.04, "Access Management for DoD Information Systems," September 3, 2024
(c) DoDI 5015.02, "DoD Records Management Program," February 24, 2015
(d) DoD CIO Memorandum, "Accelerating Adoption of Identity, Credential, and Access Management," November 26, 2024 (CUI)
(e) DoD CIO Memorandum, "Implementation of Enterprise Identity, Credential, and Access Management on the DoD Secret Fabric," August 5, 2025

This memorandum directs Department-wide implementation of automated Identity, Credential, and Access Management (ICAM) workflows for requesting, authorizing, and provisioning access to Department of War (DoW) systems and applications. This transition will replace the legacy System Authorization Access Request (SAAR) process using DD Form 2875, which has resulted in delays and data-quality issues. ICAM workflows offer a secure, policy-compliant, and modern approach that align with DoW Zero Trust and Digital Modernization objectives. In support of this initiative, DoW Components will:

- **Streamline Access**: Implement ICAM-integrated SAAR workflows that automate the provisioning of low-risk, default access and mission-standard roles based on authoritative attributes from the Enterprise Identity Attribute Service and Attribute-Based Access Control policies in accordance with References (a) and (b), requiring sponsor/data-owner attestation only when attributes are insufficient (e.g., for privileged roles or classified data), and continuously re-evaluate/revoke access based on attribute changes.

- **Enforce Governance and Auditability**: All access-related actions (requests, approvals, modifications, de-provisioning) must be captured, recorded, and stored as official records in accordance with DoW records management policy and Reference (c). Components may use Identity Governance & Administration (IGA) / Automated Account Provisioning (AAP) services that apply DoW-approved electronic signatures or system-enforced attestations, maintain immutable audit records, enforce verification requirements (need-to-know, clearance levels, segregation of duties), and provide audit feeds/dashboards for DoW oversight.

- **Maintain Enterprise Integration Through Standardized Services**: Integrate ICAM workflows with enterprise services, including Enterprise Identity Attribute Service, Defense Information Systems Agency (DISA) Enterprise Identity Services feeds, and approved Enterprise ICAM providers, to ensure consistent and interoperable identity and access management across the DoW.

- **Reporting Requirements**:

  - ICAM Service Providers will report quarterly (directly or via Application Programming Interfaces (API)) on integration and provisioning rates and timeliness, waiver requests, and access-related audit findings. The DoW CIO will use this data to assess compliance, identify obstacles, and guide policy development.

  - By June 30, 2026, DoW ICAM Service Providers must ensure that automated SAAR workflows are made available to system and application owners through an approved ICAM AAP / IGA capability to support adoption by systems that have completed ICAM onboarding.

  - By September 30, 2026, all access requests for systems and applications that have onboarded to a DoW-approved ICAM Service Provider should be processed through an automated SAAR workflow.

  - By September 30, 2027, all systems and applications must have adopted a DoW-approved ICAM Service Provider in accordance with Reference (d) and (e), all access requests must be processed through an automated SAAR workflow, and all manual authorization processes utilizing DD Form 2875 must be fully decommissioned, except where approved under a DoW Exception to Policy (E2P).

Detailed playbooks, flow diagrams, attribute mappings, API specifications, and E2P guidance will be provided in the *ICAM SAAR Workflow Implementation Guide*, which will be made available on the CIO Library at https://dodcio.defense.gov/Library/ and DISA Enterprise ICAM SharePoint site https://dod365.sharepoint-mil.us/sites/DISA-ICAM. Performance targets for provisioning timelines and automation rates will be established in the ICAM SAAR Workflow Implementation Guide and monitored through quarterly ICAM governance reporting.

Timely implementation is critical to readiness, cyber risk reduction, and modernization. Systems unable to implement an automated account provisioning capability within the implementation timelines must submit a transition plan and request an E2P using the E2P process at the DoW E2P Portal at https://rmfks.osd.mil/DoDE2P.

My point of contact for this matter is Mr. Tyler Harding at (b) (6) or via email at (b) (6) r the DoW CIO ICAM team at (b) (6)
(b) (6)

MCKEOWN.DAVI
D.W.(b) (6)
Digitally signed by
MCKEOWN.DAVID.W.(b) (6)
(b) (6)
Date: 2025.12.19 10:23:44
-05'00'

David W. McKeown
DoW Chief Information Security Officer