CLEARED
For Open Publication

Jan 20, 2026

2

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD ICAM Workflow Implementation Guide: Automated Account Provisioning and Access Governance

January 20, 2026

Version 1.0

This guide defines the technical and operational approach for automating user and administrator account provisioning, authorization decisions, and access lifecycle management using authoritative attributes and enterprise governance workflows.

UNCLASSIFIED

TABLE OF CONTENTS

Introduction

This guide supports the DoW CIO Memorandum, "Modernizing System Access Authorization Requests (SAAR) and Account Provisioning through Identity, Credential, and Access Management Workflows," dated December 19, 2025. It provides implementation guidance for transitioning the Department from the legacy DD Form 2875, System Authorization Access Request, to automated, enterprise access provisioning and access governance workflows.

This transition replaces manual, paper-based authorization processes with automation-first, attribute-driven decisioning for user and administrator access. Authoritative data sources are used to provision, modify, and revoke access throughout the account lifecycle, while human approvals are applied only when required to validate purpose, risk, or exception conditions. This approach improves operational efficiency, strengthens security, and enables consistent, auditable access controls across the enterprise.

Background

The legacy DD Form 2875 process relies on manual data entry, sequential approvals, and static documentation that do not scale to modern operational demands. These practices introduce unnecessary delays, data-quality issues, and audit challenges. The CIO Memorandum directs the use of enterprise access governance and automated account provisioning capabilities to address these shortcomings and align access management with Zero Trust principles.

Purpose

This guide provides technical and operational direction for implementing automated account provisioning and access governance across the DoW enterprise, including the use of authoritative attributes, policy-based approvals, and continuous access lifecycle management.

Scope

This guidance applies to all DoW personnel engaged in access management activities and requires enterprise-wide compliance from the following stakeholders:

- Supervisors and Sponsors reviewing access and role requests,
- IT/Cybersecurity teams managing system access controls,
- Information System Owners and Data Owners authorizing access privileges,
- System administrators creating and configuring user accounts,
- Security and compliance officers assessing access controls, and
- All DoW end users requesting system access authorization.

MINIMUM REQUIREMENTS

This implementation guide provides basic guidance for deploying DoW-wide solutions for automating the account provisioning and deprovisioning process. The guide will be updated as technical capabilities expand and ICAM Service Provider (SP) maturity increases to accommodate legacy system architectures. The broader goal is to provide standardized, secure, and compliant access management practices while maintaining operational effectiveness and mission readiness. All automated SAAR workflows implemented under this guidance will:

- ➢ Utilize authoritative attribute stores: Connect to authoritative sources for identity and attribute data (e.g., DISA, DMDC) to validate user information. Specific Application Programming Interfaces (API) and Infrastructure as Code (IaC) should be identified and used.
- ➢ Integrate with Enterprise ICAM Services: Connect to and utilize DoD-approved ICAM Service Providers, Enterprise Identity Attribute Services, and DISA identity feeds to ensure interoperability (Identity APIs and IaC to be used).
- ➢ Automate the Full Lifecycle for Joiner, Mover, and Leaver events: Workflows must manage access from initial onboarding (Joiner), through role changes (Mover), to separation (Leaver). Leaver accounts must be disabled within 24 hours of separation notification. Appropriate APIs and IaC must be identified and used to execute these actions.
- ➢ Enforce Risk-Based Approvals: Automate approvals for low-risk, default access based on user attributes. Require manual, system-enforced attestations from a sponsor or data owner only for privileged access or in cases where attributes are insufficient to determine eligibility.
- ➢ DCO integration: Generate telemetry and logs for every action within the workflow (request, approval, provisioning, modification, de-provisioning) to support Defensive Cyber Operations (DCO) and continuous monitoring.
- ➢ Report on Key Performance Indicators (KPIs): The system must be capable of collecting and reporting on key metrics to measure efficiency and security.
- ➢ Ensure a positive User Experience: The interface and functionality must be Section 508 compliant for accessibility. The interface must be intuitive and require minimal training for users submitting requests. Workflows should be configurable to allow for process improvements.

IMPLEMENTATION STRATEGY

This guidance provides basic guidance for deploying DoD-wide solutions for automating the account provisioning and deprovisioning process. The guide will be updated as technical capabilities expand and ICAM Service Provider (SP) maturity increases to accommodate legacy system architectures. The broader goal is to provide standardized, secure, and compliant access management practices while maintaining operational effectiveness and mission readiness. The implementation strategy encompasses four key components:

- **Phased Deployment** - Gradual rollout across DoW enterprise, training and transition periods provided, and progressive implementation to minimize disruption
- **Risk-Based Prioritization** – High risk system implemented first, your systems may be prioritized based on mission criticality, and timeline depends on your organization's risk assessment
- **Continuous Integration** – Ongoing updates and improvements, regular feedback incorporation and adaptive implementation based on lessons learned
- **Enterprise Standardization** – Uniform practice across the DoW components, consistent procedures regardless of location or unit, and standardized tools and processes

SAAR WORKFLOW

The approval process for provisioning access to an information system can vary based on mission need, data sensitivity, and other legal / compliance factors.

- For **System Owners**: Your primary job is to make your system "automation-ready" by connecting it to the enterprise ICAM service.
- For **ICAM Service Providers**: Your responsibility is to deliver the end-to-end automated workflow described in the guide.

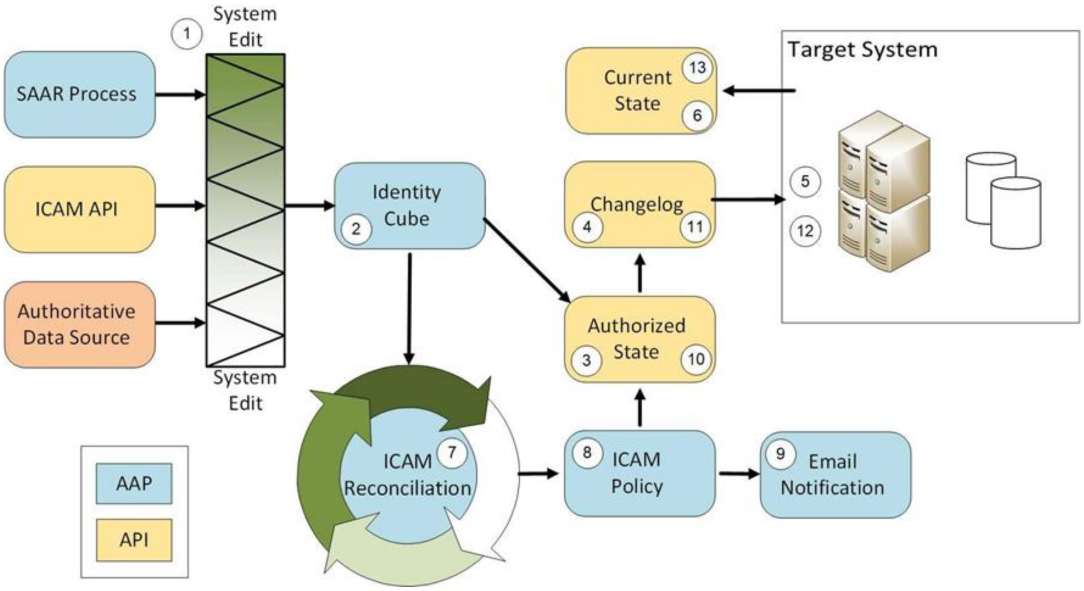

Figure 1: Example Attributes Standard Flow

Item	Description
1. System Inputs and Edits SAAR Process	Field Name and System Edit on the AAP
1. System Inputs and Edits ICAM API	Target System Read or Write via API
1. System Inputs and Edits Authoritative Data Source	Automated Input from authoritative data sources
2. AAP Identity Cube Update	Aggregation rule for attribute update into the AAP Identity Cube
3. API Authorized State	Aggregation from the AAP Identity Cube into the MUR Authorized State (Update)
4 API Changelog Notification	Changelog syntax for attribute update into the Target System Update (Update)
5. Target System Update	Target System Update method to be determined by the MP
6. API Current State	Target Application Update Handshake (Target System Update)
7. Reconciliation	Policy Reconciliation process
8. Policy – IA Training Date	The defined Policy to be enforced on the attribute.
9. Email Notification Policy	Email notification in support of the attribute Policy
10. API Authorized State	Aggregation Action for Policy Administration (Update)
11. API Changelog Notification (Update)	Changelog syntax for attribute update into the Target System Update based on Policy Administration Action
12. Target System Update	Target System Update method to be determined by the MP
13. API Current State	Target Application Update Handshake (Target System Update)

SIMPLIFIED STEP-BY-STEP GUIDE TO INITIATING A NEW ACCESS REQUEST WITH ICAM ENHANCED WORKFLOWS

Step 1: Initiate & Define the Request

Trigger: An event such as a new hire, role change, or transfer is detected in an authoritative HR or personnel system, or a preparer initiates a request by selecting a user's identity.

Action 1: Identify the User - The preparer selects the user's identity from the integrated authoritative identity source/repository, which is the DMDC PDR (or services like it).

Action 2: The Real-Time Pre-flight Check - The moment the identity is selected, the system performs an automated "pre-flight check" by querying authoritative data sources (e.g., the PDR for personnel data, NBIS for background investigation-type and clearance, and a LMS for IA (CAT) training).

The system pulls and displays the user's critical attributes, such as:

- Clearance Level and Status
- Citizenship
- Information Assurance (IA) Training Completion Date
- Current Billet/Role
- The user interface provides immediate visual feedback on these prerequisites, often with green checkmarks for valid attributes and red flags for expired or insufficient ones.

Crucially, if a non-negotiable prerequisite is not met (e.g., expired IA training), the system provides a clear error message and halts the request. This "fail-fast" approach ensures that invalid requests are stopped instantly, saving time for all subsequent reviewers.

Action 3: Define the Access Needed - Assuming the pre-flight check is successful, the preparer then defines the specifics of the access request.

- The preparer selects the target system(s) and the specific role(s) or privileges the user needs.
- The system may intelligently filter the available options. For example, it would not display roles requiring a Top-Secret clearance to a user who was just validated as having a Secret clearance.

At the end of Step 1, the system has, at a minimum, successfully gathered and validated two key pieces of information: the user's verified attributes and the specific access being requested. This complete package is then passed on to Step 2 for automated policy evaluation.

Step 2: Access Justification & Policy Enforcement

This step is designed to act as the "brain" of the operation, where the system makes an instant, policy-based decision on the access request submitted from Step 1.

Trigger: This step is triggered automatically once Step 1 is successfully completed and the access request package (containing the user's verified attributes and the requested access) is submitted.

Action 1: Automated Policy Evaluation

- The ICAM workflow evaluates the request package against the defined access requirements for the target system.
- Initially, this evaluation will most likely be based on Role-Based Access Control (RBAC) models. The workflow will mature towards a true Attribute-Based Access Control (ABAC) model as enterprise data tagging standards and richer attribute sources become available from CDAO, Data Owners, and the ICAM service providers.

Action 2: The Automated Decision - Based on the evaluation, the system makes an instant decision and directs the workflow to one of two paths:

- Outcome A: Fully Automated Approval (The "Happy Path"): If the request meets the criteria for low-risk or default access (e.g., the user has the required role attribute), the request is automatically approved. It bypasses manual review and is sent directly to Step 4 (Provisioning).
- Outcome B: Escalation for Manual Review: If the rules require a human decision (e.g., for privileged access or an exception), the request is flagged and routed to Step 3 for manual attestation.

At the end of Step 2, the system has applied the currently configured business rules to either approve the request or escalate it for necessary human review.

Step 3: Manual Attestation for High-Risk & Exception Handling

This step is the exception path, providing the essential human-in-the-loop for the most sensitive or unique access requests.

Trigger: A request is flagged for manual review by the policy evaluation in the previous step.

Action 1: Automated Routing to Approvers

- The system uses organizational data from authoritative sources to automatically route the flagged request to the appropriate approver's queue.
- The workflow can be configured to route to different individuals based on the nature of the request:
    - Supervisor: For attesting to the user's business need-to-know.
    - Information System/Data Owner: For approving access to sensitive data or systems.

Action 2: Manual Review and Attestation

- The designated approver receives a notification and reviews the details of the request within the ICAM system.
- Important Sequencing: A manual review by a Security Manager, if required, occurs only *after* the user's direct supervisor has attested to the business need.

Action 3: The Manual Decision - After reviewing, the approver takes a definitive action in the system:

- If Approved: The attestation is digitally recorded, and the approved request is sent to Step 4.
- If Denied: The request is terminated, and a notification is sent to the originator with the reason for denial.

At the end of Step 3, a final, auditable decision has been made on a high-risk request, allowing it to either proceed for provisioning or be stopped.

Step 4: Automated Provisioning & Auditing

This step is where the access is actually granted in the target system in a secure, repeatable, and fully auditable manner.

Trigger: An approved access request is received, either from Step 2 or Step 3.

Action 1: Automated Account Action (Push Provisioning)

- Upon receiving an approved request, the ICAM system's provisioning component executes the action.
- The ICAM system sends a secure command via an Application Programming Interface (API) to the target application. This is known as a "push" model.
- This command instructs the target application to Create or Modify an account, assigning the specific roles defined in the request.

- Note: Legacy "pull" models, where an application periodically downloads a list of users, are discouraged.

Action 2: Immutable Audit Trail Generation - Simultaneously, a detailed, immutable audit log is generated for the entire transaction, capturing the who, what, and when of the request, approval, and provisioning action.

Action 3: User Notification - The system sends an automated notification to the end user, confirming that their access has been successfully provisioned.

At the end of Step 4, the user has been granted the exact access they were approved for, and the entire process has been securely logged.

Step 5: Continuous Monitoring & Lifecycle Management

This is an ongoing process designed to ensure that a user's access rights remain appropriate and are updated based on changes to their status.

Trigger: This is a continuous process that begins when access is provisioned and ends when it is terminated.

Action 1: Continuous Attribute Monitoring ("Mover" Events)

- The ICAM system monitors authoritative data sources (e.g., DMDC PDR/EIAS) for any changes to a user's attributes.
- As ICAM capabilities mature towards a full ABAC implementation, these "Mover" events (e.g., a change in billet, organization, or clearance) will increasingly trigger an automatic re-evaluation and modification of a user's access rights based on policy. In the near term, these events may trigger alerts for manual review.

Action 2: Automated Deprovisioning ("Leaver" Events)

- This action is triggered when the system detects a "Leaver" event in an authoritative source (e.g., separation, end of contract).
- Upon detection, the system immediately initiates a deprovisioning workflow to disable or delete the user's account via API.
- Requirement: User accounts must be disabled within 24 hours of the official separation notification.
- This action is also captured in the immutable audit log.

At the end of this lifecycle, the system ensures that user access is managed throughout their entire tenure, automatically removing access when it is no longer needed.

IMPLEMENTATION TIMELINE

This section provides actionable guidance for implementing automated ICAM workflows. The timeline is anchored to the publication date of this guide (T-0). These dates are fixed because they are part of the formal CIO memorandum, available via the DoW CIO Library at https://dowcio.war.gov/Library/.

Phase 1: Initiation (0-180 days)

Milestone 1.1: ICAM Service Provider Onboarding

Objective: Connect all systems/applications to a DoW-approved ICAM Service Providers

Actions Required:

- Inventory all existing systems and applications requiring access management
- Identify and engage with DoW-approved ICAM Service Providers
- Establish technical connections between systems
- Pilot Implementation (test workflows and account provisioning functionality)

Key Deliverables & KPIs:

- System Inventory Completion (% of systems inventoried and quantity-#'s).
- ICAM Provider Integration Rate (#'s and % of in-scope systems connected).
- Pilot Implementation Success Rate (%).

Milestone 1.2: Automated SAAR Workflow Definition

Objective: Design and configure automated enterprise-level workflows in approved ICAM AAP/IGA capabilities

Actions Required:

- Map business authorization requirements to modern ICAM workflows and ABAC policies.
- Define attribute-based access control (ABAC) rules for auto-provisioning
- Configure sponsor/data-owner attestation requirements for high-risk access
- Establish continuous re-evaluation processes

Key Deliverables & KPIs:

- Workflow configuration documentation.
- ABAC rule definitions (# of required **roles** with defined policies).
- Attestation requirement matrices.

Phase 2: Intermediate (180 days - June 30, 2026)

Milestone 2.1: Production

Objective: Begin processing access requests through automated workflows for an initial set of prioritized systems, establishing a baseline for enterprise performance.

Actions Required:

- Identify and schedule the first wave of systems for automated workflow deployment.
- Establish and deliver training programs for personnel involved with these initial systems/applications.
- Monitor and adjust initial workflow configurations based on real-world results and user feedback.
- Document initial lessons learned and best practices to inform the scaled rollout.

Key Deliverables & KPIs:

- Initial Automation Rate (%) for the first wave of production systems.
- Initial Mean Time to Provision (MTTP) and Mean Time to Deprovision (MTTD) benchmarks.
- User Training Completion Rate for personnel associated with the initial systems.

Milestone 2.2: Scaled Deployment

Objective: Achieve 50% of adoption of automated workflows across all in-scope systems and continue to mature the access control architecture.

Actions Required:

- Expand automated workflows to additional systems and Components based on the established prioritization.
- As enterprise capabilities mature, move from simple RBAC to progressively implementing and integrating with ABAC architectural components.
- Develop component-specific implementation guides and support materials as needed.

Key Deliverables & KPIs:

- Enterprise Automation Rate (%): The percentage of access requests processed without manual intervention across all onboarded systems.

- Enterprise MTTP & MTTD: The average time for provisioning and deprovisioning across the enterprise.
- Orphaned & Dormant Account Rate: The percentage of accounts that are no longer associated with an active user.
- Privileged Access Adoption: The rate of adoption for Just-in-Time (JIT) and Just-Enough-Access (JEA) for privileged roles.
- Audit Finding Remediation: The mean time to close access-related audit findings.
- Exception to Policy (E2P) POAM Status.

Phase 3: Completion (July 1, 2026 - September 30, 2027)

Milestone 3.1: Finalize Transition of Remaining Systems to ICAM Workflow

Objective: Complete transition to automated ICAM processes.

Actions Required:

- Migrate remaining systems to automated workflows.
- Decommission paper and PDF authorization processes.
- Archive legacy authorization records appropriately.
- Conduct final validation of automated processes

Milestone 3.2: Sustainment and Optimization

Objective: Transition the automated SAAR capability from a project-based implementation to a steady-state, operational service that is continuously monitored and optimized.

Actions Required:

- Formalize long-term support structures for end-users and application owners.
- Establish a governance process for reviewing and updating ABAC policies and workflows based on performance data and new requirements.
- Monitor technology roadmaps and plan for future capability enhancements and component refreshes.

Key Performance Indicators (KPIs):

- User Satisfaction Scores (e.g., via periodic surveys).
- Policy Optimization Rate: The frequency at which ABAC policies are reviewed and updated.
- Long-Term Trend Analysis of all previously established KPIs (MTTP, Automation Rate, etc.).

Note: This guide recognizes the value of future enhancements, such as fast-track access requests for users with existing baseline credentials, which will be considered in subsequent updates.

REFERENCES

The following resources provide additional DoD ICAM reference materials, technical standards, and component-specific guidance.

Governing DoD Instructions

DoD Instruction 8520.03, Identity Authentication for Information Systems

- This instruction establishes policy for identity authentication and is a foundational component of the overall ICAM strategy.

DoD Instruction 8520.04, Access Management for Information Systems

- This instruction establishes policy and assigns responsibilities for managing access to DoD information systems. It is the primary policy driver for this implementation guide.

Federal & NIST Technical Standards

Federal Identity, Credential, and Access Management (FICAM) Architecture

- This document outlines the U.S. Government's overarching strategy and framework for ICAM, providing the strategic context for the DoD's implementation.

NIST Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management

- Provides the detailed technical guidelines for managing digital identities throughout their lifecycle, including the provisioning, maintenance, and deprovisioning processes discussed in this guide.

NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations

- This is the foundational standard for ABAC. It defines the architecture and components that are the target state for this implementation.

DoD Enterprise & Component Resources

DISA Enterprise ICAM (E-ICAM) SharePoint Site

- Provides the primary portal for enterprise-level ICAM guidance, services, and contacts.
- https://dod365.sharepoint-mil.us/sites/DISA-ICAM

U.S. Army ICAM Portal

- Provides guidance and resources specific to U.S. Army implementations.
- https://icamportal.us.army.mil/

Department of the Navy ICAM Site

- Provides guidance and resources specific to Department of the Navy implementations. (PKI-enabled)
- https://digital.navy.mil/nis

Department of the Air Force CIO Site

- Provides guidance and resources specific to Department of the Air Force implementations.
- https://www.dafcio.af.mil/

DAF API Reference Architecture

- Provides the technical standards and best practices for building secure and interoperable APIs. It serves as a valuable model for all DoD Components.
- https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20API%20Reference%20Architecture%202.0.pdf