DOPSR 26-P-1206

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

August 14, 2026

Version 2.0

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.

TABLE OF CONTENTS

INTRODUCTION

This guide supports the Department of War (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 foundational implementation guidance for transitioning the Department from a manual, form-centric process, specifically the legacy DD Form 2875, "System Authorization Access Request" (SAAR) form, to attribute-centric, automated access provisioning and governance workflows.

To accomplish this, the guide introduces the strategic framework of Identity Lifecycle Management (ILM), which is executed through tactical tools such as Automated Account Provisioning (AAP) workflows. This transition replaces paper-based authorization with automation-first, attribute-driven decisioning. 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.

This revised guide acknowledges that many changes to a specific user's access and entitlements are clustered around joiner-mover-leaver events. A specific user might go through onboarding as a new member of the DoW, for example, or onboard to a new organization or site via a Permanent Change of Station (PCS) move or detail. This guide advocates leveraging automated provisioning to advance the user experience for servicemembers, civilians, and contractors by reducing bureaucracy using existing Department processes and data. DoW applications and systems will need to onboard to ICAM services to reduce no-value-add steps.

Governed Access, Zero Trust, and Auditability

Automated Account Provisioning (AAP) workflows should be implemented as governed lifecycle control mechanisms, not only as request-routing or provisioning tools. Onboarding applications and systems to AAP supports Department Zero Trust implementation by enabling least privilege, need-to-know/right-to-know enforcement, conditional access, user inventory, authoritative attribute use, lifecycle revocation, continuous monitoring, and auditable policy enforcement. The same policy basis used to grant or modify access should also support access suspension, deprovisioning, reconciliation, and audit.

AAP workflows may also function as governed sources of identity data when enterprise authoritative sources do not yet capture the mission or business context needed for access decisions. For example, a workflow may create, update, or revoke a managed

group membership, member of ( ) attribute, sponsorship status, onboarding status, mission assignment, welcome-center completion, or other approved eligibility indicator. Any workflow-created identity or eligibility attribute should have a defined owner, meaning, authoritative or workflow source, quality expectation, review cadence, revocation trigger, and audit trail.

This guide recognizes that certain access is assigned automatically based on a user's organizational role, affiliation, or lifecycle state. Within the Department, such pre-approved automated access shall not be treated as unconditional, permanent, or unmanaged. This access must remain strictly scoped to mission or business need, owned by a Resource Owner, version-managed, auditable, and revocable through Joiner-Mover-Leaver events, attribute changes, or owner action.

For systems that support financial reporting, financial transactions, feeder processes, or internal controls over financial reporting, AAP workflows also support audit readiness by producing repeatable evidence of access authority, approval, provisioning, modification, deprovisioning, reconciliation, and control operation. This evidence should be retained consistent with applicable records management and financial statement audit requirements.

Background

The legacy DD Form 2875 process relies on manual data entry, sequential approvals, and static documentation that does 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 AAP 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 DoW-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.

ROLES AND RESPONSIBILITIES

Successful implementation of automated workflows requires a clear understanding of roles and responsibilities.

- ICAM Service Providers (SPs): Are responsible for developing, deploying, and maintaining the standardized AAP workflows, including bundled and dedicated workflows. They act as the technical implementers of the automation strategy.

- Resource Owners (ROs): Retain ultimate authority over who is granted access to their systems. ROs are responsible for defining the access requirements (e.g., training, clearance checks), determining the risk level of their system, and concurring on the appropriate workflow (bundled or dedicated) to be used.

- Director of National Intelligence (DNI) / Committee on National Security Systems (CNSS): Continue to set the overarching policy framework for access to classified information and National Security Systems (NSS). This guide provides the implementation strategy to execute those policies in an automated fashion.

IMPLEMENTATION STRATEGY

This guidance provides foundational guidance for deploying DoW-wide solutions to automate the account provisioning and deprovisioning process. It accomplishes this by describing the strategic framework of Identity Lifecycle Management (ILM), which is executed through tactical tools such as Automated Account Provisioning (AAP) workflows.

Identity Lifecycle Management (ILM) is a security framework for managing a user's access to technology resources throughout their entire tenure with an organization. It applies to both human users, like civilians, military personnel, and contractors, and non-human entities, such as applications and services. The core purpose of ILM is to ensure that the right individuals have the appropriate level of access at all times, which enhances security, boosts operational efficiency, and helps maintain regulatory compliance.

The ILM process is commonly structured around the "Joiner, Mover, Leaver" (JML) model.

- The "Joiner" phase involves onboarding new users by creating their digital identities and provisioning the necessary access rights based on the principle of least privilege.

- The "Mover" stage addresses changes in a user's role, such as a promotion or transfer, by updating their access permissions accordingly to prevent the accumulation of excessive privileges, a risk known as "privilege creep."

- Finally, the "Leaver" phase handles offboarding by promptly and securely deprovisioning all access when a user leaves the organization, which mitigates security risks from lingering or orphaned accounts.

By implementing a robust ILM strategy, often automated through Identity Governance and Administration (IGA) solutions, ICAM Service Providers can significantly strengthen their security posture. This system ensures that access is granted just-in-time, modified as roles change, and revoked immediately upon departure. This not only protects sensitive data but also streamlines IT and HR workflows, reduces manual errors, and creates a clear audit trail essential for meeting compliance standards, like CUI. 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 and Automation Eligibility:** Systems, applications, entitlements, and bundles should be prioritized based on both access risk and automation readiness. The presence or absence of a human approval step is not, by itself, the measure of risk. Access may be eligible for automated approval when the Resource Owner or bundle owner has pre-approved the access conditions; eligibility can be determined using authoritative or governed attributes; the policy is version-managed and auditable; and the same policy basis supports provisioning, modification, suspension, deprovisioning, reconciliation, and review.

- **Low-Risk / Automated Pre-Approved Access:** Low-Risk access is access that can be granted through a fully automated process because the eligibility criteria are objective, pre-approved, governed, and verifiable through authoritative or governed attributes. Such access must remain scoped to mission or business need, owned by a Resource Owner or bundle owner, auditable, lifecycle-managed, and revocable through JML events, attribute changes, owner action, certification outcomes, or exception expiration. A system is only considered low risk if its access can be granted without a "human in the loop" for approval. Provisioning is

fully automated based on a Resource Owner's pre-approved conditions, which are met when a user possesses a specific set of verifiable, authoritative attributes.

- **Moderate to High-Risk / Enhanced Evaluation Access:** Access should be treated as moderate to high-risk when it requires subjective judgment, mission-specific validation, additional legal or compliance checks, elevated privilege, access to sensitive data, or enhanced accountability. High-risk access includes, but is not limited to:

- Need-to-Know validation.
- Non-Disclosure Agreement (NDA) requirements.
- clearance checks.
- privileged or administrator-level roles.
- unique mission.
- OPSEC, or security controls.
- segregation-of-duties or toxic-combination concerns.
- access supporting financial reporting, financial transactions, feeder systems, or internal controls over financial reporting.
- access that can modify identity, access, audit, security, or workflow controls.
- bulk export or sensitive data access.
- emergency or break-glass access.
- non-human identities or persistent integrations.
- access based on stale or non-authoritative attributes; and
- access with material cost, licensing, or resource-consumption impacts.

  Note: Manual validation steps for these requirements (such as a manual clearance or Need-to-Know check) shall only be utilized as an interim exception when an automated, attribute-driven policy check is not technically feasible.

- **Bundling Implication:** A resource may be included in a low-risk bundle only when it shares the same governed eligibility criteria, authoritative or governed attribute checks, lifecycle triggers, revocation logic, reconciliation expectations, and

Resource Owner or bundle owner concurrence. If a resource introduces additional risk indicators, different approval logic, SoD or toxic-combination concerns, different revocation triggers, or unique audit requirements, it should be moved to a higher-risk bundle or dedicated workflow.

- **Continuous Integration** – Ongoing updates and improvements, regular feedback incorporation and adaptive implementation based on lessons learned.

- **Enterprise Standardization –** This promotes uniform practices and consistent procedures across the DoW components. Standardized interfaces also promote modularity and support evolutionary modernization. The Bundled AAP Workflow advances these goals.

RULES OF BEHAVIOR AND ACCEPTABLE USE POLICY (AUP)

To satisfy NIST SP 800-53, Planning (PL) Control 4 (PL-4) requirements for Rules of Behavior, AAP workflows should integrate the delivery and electronic signature of User Agreements, Warning Banners, and acceptable use policies. Each Bundled AAP Workflow owner or component authority may tailor these agreements to meet specific enterprise, business, or mission requirements. The workflow may deliver these for signature directly or validate them in conjunction with mandatory Cybersecurity Awareness Training. The completion of this agreement should be recorded as a distinct, e-signed, and version-controlled enterprise attribute that can be queried by any downstream application or bundle to verify compliance prior to granting access.

HANDLING EXCEPTIONS AND NON-AUTOMATED SYSTEMS

The DoW recognizes that not all systems can be integrated into a fully automated AAP workflow immediately. Systems may be technically incompatible or require unique, manual review processes that cannot be automated. In such cases, ICAM SPs and Resource Owners must document these exceptions and continue to use the existing manual SAAR process (DD Form 2875) as an interim measure.

To utilize this interim measure, the Resource Owner must submit a formal Exception to Policy request, package-endorsed by their Component CISO and formally approved by the DoW CIO (or designated authority). To ensure manual processes do not become unmanaged permanent alternatives, each exception requires formal governance. The exception documentation must identify an owner, business or mission justification, an expiration or review date, compensating controls, a manual provisioning and revocation procedure, a reconciliation cadence, and a modernization path. Where appropriate, the exception should be linked to a Plan of Actions & Milestones (POA&M). Manual SAAR or

DD 2875 processes used as interim measures must still support timely JML-driven revocation, access suspension, periodic review, and Resource Owner accountability.

BUNDLED AAP WORKFLOWS:

A bundled AAP workflow allows an ICAM service provider to use one automated workflow to provision or deprovision access to multiple resources, but only when all resources require the same decisions and the same authoritative-attribute checks.

Bundled AAP workflows can be created for resources with a shared risk profile, whether low-risk or high-risk, as long as the criteria for the bundle are clearly defined.

- Low-Risk Bundles are for resources that can be granted through a fully automated process with no human approval. A resource is considered low-risk if, and only if, access can be granted through a fully automated process without a "human in the loop" for approvals.
- High-Risk Bundles group resources that require an identical manual approval workflow with additional requirements (e.g., additional attribute checks, new approvals, or elevated risk).

If a resource's access requirements change, it must be moved to a bundle that matches its new risk profile or be removed from bundling entirely. All resources within a given bundle must always share identical logic and validation processes.

Example

An ICAM Service Provider may create a Bundled AAP Workflow for applications that require only:

- Current Cyber Awareness / IA training, and
- Electronic AUP acknowledgement.

Any resource that requires **additional** checks—such as clearance or Need-to-Know (NTK) validation, privileged role approval, or SoD review—**cannot** be included in the bundle.

Bundled Automated Account Provisioning (AAP) Workflow Requirements

A resource may be included in a bundled workflow **only if all** the following conditions are true:

1. **Version-Controlled Authorization Profile:** Each Bundled AAP Workflow must maintain a version-controlled authorization profile that documents ownership, mission or business purpose, included entitlements, eligibility criteria, prerequisite attributes, authoritative sources, approval logic, revocation triggers, review cadence, exception path, and cost or licensing considerations. Changes to the profile should be reviewed, assigned an effective date, retained for auditability, and reconciled with the implementation in the ICAM/AAP capability.
2. **Same decision logic:**
   The resource uses the same routing and approvals as the Bundled AAP Workflow (no extra approvers or conditional logic).
3. **Same authoritative attribute validations:**
   The resource relies on the same prerequisite attributes pulled from the same authoritative sources (e.g., IATrainingCurrent = true; AUPAttested = true).
4. **Same risk posture:**
   All resources in the bundle share the same risk level. For example, a low risk bundle would not include any resources requiring enhanced controls like clearance checks, while a high-risk bundle would group only those resources that share the exact same enhanced controls and approval requirements.
5. **Resource Owner concurrence:**
   The Resource Owner agrees that the resource meets the criteria and will use the workflow for routine grants, while still retaining full approval authority over any sensitive or high-risk access.

If **any** requirement is not met, the resource **must use a separate AAP Workflow.**

NOTE: While bundled workflows are ideal for low-risk resources, the same principle of reusability can be applied to certain high-risk resources. A high-risk bundled workflow may be used when multiple resources share the exact same human-in-the-loop approval requirements (e.g., the same set of approvers, clearance checks, and validation steps). This allows an organization to standardize its high-risk approval processes, even though the final decision remains manual.

Workflow Outcomes: Direct vs. Attribute-Based Provisioning

A bundled workflow can conclude in one of two ways:

- **Direct Provisioning**: Upon successful completion, the workflow directly grants the user individual entitlements to a predefined list of applications. This approach is straightforward but less flexible.

- **Attribute-Based Provisioning** (Recommended): Upon successful completion, the workflow grants a single, reusable attribute to the user's identity profile. This attribute certifies that the user has met a specific set of requirements. This method is highly recommended as it allows new applications to be added to the bundle in the future; they can simply check for the presence of the attribute to grant access without requiring the user to re-run the workflow.

ICAM/AAP WORKFLOWS

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

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

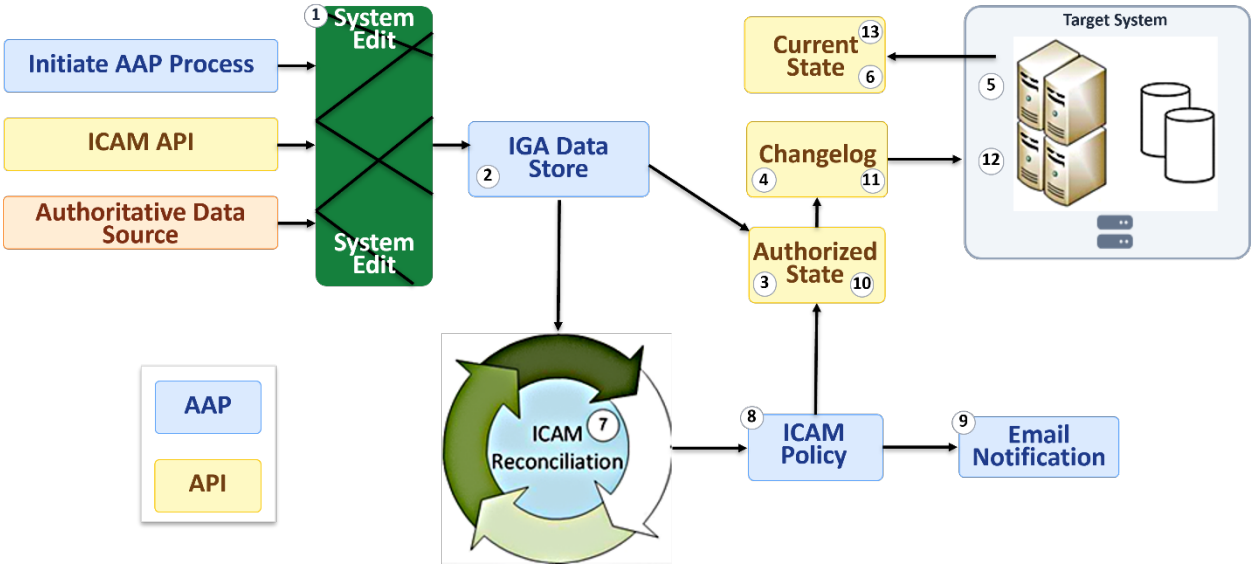

Figure 1: Example Attributes Standard Flow

Item	Description
1. System Inputs and Edits AAP 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 IGA Data Store Update	Aggregation rule for attribute update into the AAP IGA Data Store
3. API Authorized State	Aggregation from the AAP IGA Data Store into the Master Entitlement Record (MER) 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 Mission Partner
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)

INITIATING A NEW ACCESS REQUEST WITH ICAM AAP 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 an LMS for IA (CAT) training). Under Zero Trust, there shall be no "assumed" trust, reciprocity assumptions, or cached compliance states. The user's attributes (e.g., active clearance, completed training, citizenship, and signed rules of behavior) must be verified dynamically in near-real-time from the authoritative source at the initiation of the workflow and re-evaluated continuously throughout the session life-cycle.

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

a. Clearance Level and Status

b. Citizenship

c. Information Assurance (IA) Training Completion Date

d. Current Billet/Role

e. 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.

a. The preparer selects the target system(s) and the specific role(s) or privileges the user needs.

b. 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

a. The ICAM workflow evaluates the request package against the defined access requirements for the target system.

b. 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:

a. 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).

b. 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

a. The system uses organizational data from authoritative sources to automatically route the flagged request to the appropriate approver's queue.

b. 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

a. The designated approver receives a notification and reviews the details of the request within the ICAM system.

b. 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:

a. If Approved: The attestation is digitally recorded, and the approved request is sent to Step 4.

b. 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)

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

Governed Attributes and Operational Control in JML

To operationalize lifecycle-driven access, JML automation must leverage governed access-control attributes to determine whether access remains valid. Where a manager, sponsor, mission owner, Resource Owner, or business-process owner must control access, the provisioning policy should include a governed attribute (such as a managed group membership, member of ( ) attribute, sponsorship status, billet assignment, onboarding status, or in-processing status). This control attribute must be evaluated alongside enterprise ABAC attributes from authoritative sources.

This approach allows the governing authority to manage lifecycle context that may not be fully represented in enterprise ICAM attributes, such as local mission assignment, licensing limits, welcome-center completion, sponsorship, operational suspension, or out-of-band membership considerations.

Where authoritative enterprise data is unavailable, the AAP workflow itself may be used to create, maintain, or update these governed control attributes. In these scenarios, the business or mission owner must define the meaning, quality expectations, ownership, review cadence, and revocation triggers for the attribute, consistent with ICAM attribute standards. This ensures parity across RBAC, ABAC, and entitlement-management patterns by making the access condition explicit, auditable, and lifecycle-managed.

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)

a. The ICAM system monitors authoritative data sources (e.g., DMDC PDR/EIAS) for any changes to a user's attributes.
b. 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)

a. This action is triggered when the system detects a "Leaver" event in an authoritative source (e.g., separation, end of contract).
b. Upon detection, the system immediately initiates a deprovisioning workflow to disable or delete the user's account via API.

c. Requirement: User accounts must be disabled within 24 hours of the official separation notification.
d. This action is also captured in the immutable audit log.

Action 3: Closed-Loop Reconciliation and Certification

a. Authorization is not complete at provisioning. The authorized state in the ICAM/AAP capability must be continuously compared with the current state in target systems.
b. Entitlement drift, out-of-band access, orphaned or dormant accounts, manually created administrator accounts, and expired exceptions must be identified and routed for automated correction or Resource Owner review.
c. Risk-based periodic access certification must be conducted for Bundled AAP Workflows, privileged access, exception-based access, and costly licensed access to confirm that the access basis remains valid and aligned with mission need.

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) Period ended January 30, 2026

Milestone 1.1: ICAM Service Provider Onboarding

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

Actions Required:

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

Key Deliverables & KPIs:

a. System Inventory Completion (% of systems inventoried and quantity-#'s).

b. ICAM Provider Integration Rate (#'s and % of in-scope systems connected).

c. Pilot Implementation Success Rate (%).

Milestone 1.2: Automated AAP Workflow Definition

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

Actions Required:

a. Map business authorization requirements to modern ICAM workflows and ABAC policies.

b. Define attribute-based access control (ABAC) rules for auto-provisioning.

c. Configure sponsor/data-owner attestation requirements for high-risk access.

d. Establish continuous re-evaluation processes.

Key Deliverables & KPIs:

a. Workflow configuration documentation.

b. ABAC rule definitions (# of required **roles** with defined policies).

c. Attestation requirement matrices.

Phase 2: Intermediate (January 30, 2026 - June 30, 2026) Period ended 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:

a. Identify and schedule the first wave of systems for automated workflow deployment.

b. Establish and deliver training programs for personnel involved with these initial systems/applications.

c. Monitor and adjust initial workflow configurations based on real-world results and user feedback.

d. Document initial lessons learned and best practices to inform the scaled rollout.

Key Deliverables & KPIs:

a. Initial Automation Rate (%) for the first wave of production systems.

b. Initial Mean Time to Provision (MTTP) and Mean Time to Deprovision (MTTD) benchmarks.

c. 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:

a. Expand automated workflows to additional systems and Components based on the established prioritization.

b. As enterprise capabilities mature, move from simple RBAC to progressively implementing and integrating with ABAC architectural components.

c. Develop component-specific implementation guides and support materials as needed.

Key Deliverables & KPIs:

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

b. Enterprise MTTP & MTTD: The average time for provisioning and deprovisioning across the enterprise.

c. Orphaned & Dormant Account Rate: The percentage of accounts that are no longer associated with an active user.

d. Privileged Access Adoption: The rate of adoption for Just-in-Time (JIT) and Just-Enough-Access (JEA) for privileged roles.

e. Audit Finding Remediation: The mean time to close access-related audit findings.

f. Exception to Policy 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:

a. Migrate remaining systems to automated workflows.

b. Decommission paper and PDF authorization processes.

c. Archive legacy authorization records appropriately.

d. Conduct final validation of automated processes

Milestone 3.2: Sustainment and Optimization

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

Actions Required:

a. Formalize long-term support structures for end-users and application owners.

b. Establish a governance process for reviewing and updating ABAC policies and workflows based on performance data and new requirements.

c. Monitor technology roadmaps and plan for future capability enhancements and component refreshes.

Key Performance Indicators (KPIs):

a. User Satisfaction Scores (e.g., via periodic surveys).

b. Policy Optimization Rate: The frequency at which ABAC policies are reviewed and updated.

c. 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 DoW ICAM reference materials, technical standards, and component-specific guidance.

DoW 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.

DoW Instruction 8520.04, Access Management for Information Systems

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

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 DoW'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.

DOW 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://armyeitaas.sharepoint-mil.us/sites/usaasc-peoc3n-i2s-eicam-service-catalog

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 DoW Components.
- https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20API%20Reference%20Architecture%202.0.pdf