How Okta can meet the DoW ICAM Workflow Implementation Guide on AAP and Access Governance

Okta Identity Governance (OIG) is built to handle the scale and security requirements of modern Department of War (DoW) operations. By leveraging real-time attributes—such as Title and Rank—Okta automates the verification process for Mission App Owners, helping to ensure that application access is always synchronized with a user's current authorized status. This architecture supports the enterprise-wide implementation of automated Identity, Credential, and Access Management (ICAM) workflows for requesting, authorizing, and provisioning access to DoW applications.

To maximize operational velocity, Okta enforces risk-based approvals. This allows for the automation of low-risk, default access based on verified user attributes, while reserving manual, system-enforced attestations from sponsors or data owners for privileged access or cases where attributes alone are insufficient. Warfighters can submit these requests via Okta, Teams, or Slack, gaining rapid access through trusted, compliant workflows. Okta for US Military delivers the core pillars of an ICAM technology stack to ensure verified access to mission-critical systems.

Mapping Okta to DoW Requirements

Use this document to see how Okta helps your organization transition from manual processes to automated, attribute-based access control. We map specific Okta capabilities to the "automation-first" requirements defined in the DoW CIO Memorandum, "*Modernizing System Access Authorization Requests (SAAR) and Account Provisioning through Identity, Credential, and Access Management Workflows*," and associated *ICAM Workflow Implementation Guide*. This breakdown provides a clear path for administrators to replace legacy SAAR paperwork with modernized, compliant ICAM workflows that prioritize both security and speed.

Minimum Requirement	Okta Alignment
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.	**Okta Universal Directory & Profile Sourcing** Consolidates data from DISA, DMDC, LDAP, Active Directory, and HR systems into a unified "Identity Cube." The Governance Engine consumes these attributes to enforce fine-grained, app-specific permissions automatically via API and Infrastructure as Code (IaC).
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).	**Proven Interoperability with DoD E-ICAM** Okta possesses extensive DoD enterprise customer experience. By leveraging its standards-based integration patterns and supporting all common attribute, governance, authentication, and authorization standards, Okta has successfully integrated with a large portion of existing Department of Defense ICAM, data, and attribute services (E-ICAM).
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.	**Okta Lifecycle Management** Automates access decisions using dynamic Role- and attribute-based access controls (RBAC and ABAC). Okta Lifecycle Management is able to facilitate all joiner, mover, leaver use cases. When a "Leaver" event is detected in the authoritative source via scheduled import or real-time attribute sync, Okta instantly deprovisions accounts across connected systems, eliminating orphan accounts and meeting the 24-hour disablement requirement.
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.	**Entitlement Management & Access Requests** Implements Separation of Duties checks to prevent conflicting entitlements. Assigns entitlements using policy for low-risk, mission-standard access (fully automated approval). For high-risk access, Access Requests conditions automates the routing of requests to resource owners, sponsors, or data owners for manual approval.
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.	**System Log & Access Certifications** Provides a detailed System Log capturing all identity-related events, which can be either pulled into other services via authentication API calls or proactively pushed used Log Streaming. Access Certifications generate ad-hoc, scheduled, and event-driven campaigns to keep risks at acceptable levels, providing a complete audit trail of who approved access, when it was granted, and how it was provisioned.
Report on Key Performance Indicators (KPIs) The system must be capable of collecting and reporting on key metrics to measure efficiency and security.	**Interactive Reports & Auditor Reporting Package** The Okta Admin Dashboard features high-level KPI charts highlighting critical security data points that impact a customer's security posture, alongside interactive reports on user access and MFA enrollment, to name a few. To further streamline compliance, the Auditor Reporting Package generates campaign-specific reports—such as 'Resource Access Changes'—to ensure complete traceability and significantly reduce manual data assembly for auditors.
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.	**Odyssey Design System** Okta ensures Section 508 and WCAG 2.2 Level AA compliance through the Odyssey Design System, which provides accessible, intuitive interfaces for Okta Identity Governance's Access Request Inbox and Access Certifications Reviewer apps. Technical findings are documented via 2025 Accessibility Conformance Reports and verified by third-party auditors to ensure a standard of inclusive digital delivery across the Okta Platform.

To learn more about how Okta for US Military can help your organization transition from legacy, paper-based processes to automated Impact Level 4 access provisioning and identity governance workflows, contact us at federal@okta.com.