Department of the Air Force Identity, Credential, and Access Management (ICAM) Strategy

Version 2.0
7 June 2021

OPR:
SAF CIO

KNAUSENBERGER.LAUREN.1538604565 Digitally signed by KNAUSENBERGER.LAUREN.1538604565 Date: 2021.06.09 23:11:48 -04'00'

LAUREN BARRETT KNAUSENBERGER, SES, DAF
Chief Information Officer

This page intentionally left blank.

Executive Summary

The Department of Defense (DOD) aims to revolutionize its network-focused defense-in-depth "castle and moat" cybersecurity strategy into one that focuses on individual data as a strategic asset, and lays the foundation for Zero Trust. To achieve this, the Department of the Air Force (DAF) must evolve towards a data-centric cybersecurity strategy with a multi-faceted Identity, Credential, and Access Management (ICAM) foundation. ICAM encompasses the full range of activities related to creation of digital identities and maintenance of associated attributes, credential issuance, authentication, which lead to access management decisions, based on authenticated identities and associated attributes.

Historically, the DAF defined and implemented ICAM principles to protect network and resource access at varying organizational levels. Several disparate initiatives have even evolved into useful maturity levels. However, to date, the DAF has failed to employ these measures uniformly and in an integrated manner across the enterprise. This lack of a consistent, standards-based approach, without centralized governance, unnecessarily increases the operational risk of compromise, reduces efficiency and effectiveness, and is fiscally unsustainable.

This strategy aims to evolve ICAM into an enterprise solution and provide the warfighter with the advantages of a complete ecosystem. The DAF envisions a centralized identity platform, with a governance framework that provides direction and guides delivery of automated enterprise authorization services that support rapid access to mission and business information, while forming the foundation for a Zero Trust Architecture. These capabilities eliminate duplication and fragmentation, mitigate internal and external threat vectors, improve the user experience, and realize significant savings.

The goal state for DAF ICAM begins with a federated and centralized management process, creating fundamental trust in the digital identities of all person and non-person entities (NPE) interacting with DAF networks, services or data. It permits multiple approved authenticators, such as Common Access Card (CAC),Fast Identity Online (FIDO2), hardware tokens, and mobile authenticators, which support various environments, users, devices, and missions. The enterprise ICAM user interface provides seamless, secure, and auditable access, automatically ensuring the right user has the right access to approved resources anytime, anywhere. It also includes automated application and enforcement of DAF ICAM policies, guidance, and standards to evolve our cybersecurity into a more resilient defense posture. By adding enterprise federation, DAF creates trusted information exchanges across services, other government agencies, allies, and other key partners.

The four main goals of this strategy and their associated objectives focus DAF resources and align with the DoD ICAM Strategy. Ultimately, this strategy evolves the current state of DAF ICAM into a more secure, efficient, and effective future state, which specifically enhances cybersecurity, interoperability, and end user access to and experience with enterprise services.

- Goal 1: Centralized Identity Management
- Goal 2: Universal Authenticator Support
- Goal 3: Seamless Enterprise Access Management Services
- Goal 4: Standardized DAF ICAM Governance Framework and Policy Enforcement

Table of Contents

This page intentionally left blank.

1 Introduction

The DoD's 2019 Digital Modernization Strategy aims to revolutionize its network-focused defense-in-depth "castle and moat" cybersecurity strategy into a Zero Trust Architecture (ZTA), that focuses on individual data as a strategic asset. Zero Trust is a data and application access strategy that assumes all connections come from untrusted sources. Access to each resource is only granted after establishing and continuously re-verifying enough confidence in the user's identity, device and context of each connection. To achieve this, the Department of the Air Force (DAF) must evolve towards a data-centric cybersecurity strategy with a multi-faceted Identity, Credential, and Access Management (ICAM) foundation. ICAM encompasses the full range of activities related to the creation of digital identities and maintenance of associated attributes, credential issuance, authentication, and making access management decisions based on authenticated identities and associated attributes. DoD began this effort in 1999 with the "DoD Public Key Infrastructure (PKI)" memorandum and subsequent 2000 DoD PKI RoadMap which established an end-state, strategy and timeline for DoD's PKI capabilities. DoD, in close coordination with the Combatant Commands, Services and Agencies (CC/S/As), developed cryptographically strong tokens (e.g., CAC) based on a complete and secure lifecycle management process - from identity proofing to token revocation. After taking this foundational step, DAF must now align with the 2020 DoD ICAM Strategy and provide the warfighter with the advantages of a complete ICAM ecosystem and pave the way for Zero Trust.

1.1 Purpose

ICAM is the cornerstone of the rock solid digital foundation that connects all Air and Space Force members across a trusted digital force. It responsibly opens the aperture on information sharing, offering new collaboration opportunities with mission and non-mission partners. This document describes the strategic concept for establishing DAF enterprise ICAM capabilities and services, based on a governance framework, to deliver real-time ability to dynamically share and use all data authorized for each user or NPE - anytime and anywhere.[1] The DAF envisions a centralized identity platform, with a governance framework that provides direction and guides delivery of automated enterprise authorization services that support rapid access to mission and business information, while forming the foundation for a DAF ZTA. These capabilities eliminate duplication and fragmentation, mitigate internal and external threat vectors, improve the user experience, and realize significant savings. These capabilities must be able to run across classification levels, without drift, meaning they provide a consistent configuration and user experience across environments, including air-gapped environments. They will eliminate duplication and fragmentation, mitigate internal and external threat vectors, improve the user experience, and realize significant savings.

[1] Fusion of DoD, FICAM, and AF ICAM vision statements

1.2 Scope

This Strategy aligns with the DoD ICAM Strategy scope and includes the full range of activities described.[2] Unless explicitly excluded in policy, this strategy applies to all DAF portions of the DoD unclassified, secret, top secret, and United States owned releasable networks and information systems under the authority of the Secretary of Air Force, including the Special Access Program (SAP) element. Information systems include those that are owned and operated by or on behalf of the DAF, including systems hosted at DAF data centers, Platform Information Technology (PIT) systems, contractor-operated systems at cleared defense contractor locations and on the AF Information Network (AFIN), cloud hosted systems, and systems hosted on closed operational or development networks, with no connection to the AFIN. New system owners should plan to incorporate and implement these strategy elements at the appropriate time in their lifecycle development and in line with other policy. DAF envisions a future state where each identity contains all the necessary attributes and entitlements for each network fabric to which access is authorized (NIPR, SIPR, JWICS, etc.), providing a consistent user experience, regardless of environment.

[2] DoD ICAM Strategy, 30 Mar 20

2 Current State of ICAM Across the DAF Enterprise

The DAF defined and implemented ICAM principles to protect network and resource access at varying organizational levels; primarily in a pre-Enterprise Information Technology (EIT) environment. The DAF is now making a concerted effort to move ICAM to an EIT environment, aligned with the DAF Enterprise IT Strategy – Key Pillars, and this involves transitioning multiple enterprise-level ICAM efforts underneath a single DAF Enterprise ICAM EIT capability. Moving DAF Enterprise ICAM to this level of EIT capability requires a consistent, standards-based approach. Without centralized ICAM governance and EIT principles, DAF incurs increased operational risk of compromise, reduced efficiency and effectiveness, and requires an unsustainable financial model to maintain.

2.1 Identity Management

Identity Management (IdM) combines the technical systems, policies, and processes which create, define, govern, and synchronize the ownership, utilization, and safeguarding of digital identities – the digital representation of a person or non-person entity (NPE). Digital identities include a unique identifier (e.g., Electronic Data Interchange Personal Identifier (EDIPI)) and a set of attribute values (e.g., marital status, duty location, rank, security clearance eligibility, etc.) about the entity.[3] Today, people can have multiple identity persona attributes, each describing a specific role and responsibility that grants them different authorities and access (e.g., active duty, guard, reserve, civilian, contractor, dependent, retiree, etc.). Identity management aims to establish a trustworthy process for assigning attributes to a digital identity and binding that identity to a person or NPE. NPEs are a physical device, virtual machine, system, service, or process that is assigned an identifier and may be issued credentials to support authentication and authorization.[4]

Today, Air Force Directory Services (AFDS) and the AF Personnel Directorate (AF/A1) are each responsible for managing DAF person identities. AFDS manages the identities and a number of associated attributes for DAF active duty military, government civilians, and contractors. AF/A1 also supports additional DAF active duty military, government civilian, and contractor attributes as well as the identities and attributes for the inactive population of retirees, dependents, and non-CAC eligible members. The DAF SAP networks maintain their own central attribute store and external departments and agencies (D/A) provide limited interoperability. AF Intelligence Community (IC) in accordance with the Director of National Intelligence (DNI) and AF/A2/6 policy and guidance manage identities and associated attributes for IC networks, systems and services.

[3] FICAM Roadmap and Implementation Guidance, v2.0, 2 Dec 2011, Section 7, Initiative 5 (pg 197)
[4] DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design (RD), DoD CIO, June 2020.

AFDS is the DAF enterprise attribute service and presents authoritative identity attributes for application-owner consumption. It currently provides an enterprise-level identity directory infrastructure for person entities (PE), as well as foundational data elements and technologies, which attempts to enable secure, timely delivery of identity data attributes required by DAF and DoD applications and organizations. AFDS draws from nine authoritative data stores[5] to create individual DAF identity accounts and provision them for Air Force Network (AFNet) activation. AFDS also offers all the capabilities and services available on NIPRNet, mirrored to customers on SIPRNet. As identity attributes change, AFDS automatically updates the identity in Active Directory (AD) with the new identity attribute information. AFDS capabilities reduce the redundancy of directory services, disparate databases, and attribute stores currently deployed across the DAF and DoD. While capabilities exist to manage person identities and their attributes, the DAF currently does not have a capability to manage the lifecycle for NPE digital identities.

AF/A1 is responsible for a portfolio of systems, which manage the 'talent' of all DAF military and civilian personnel. These portfolios include the Advanced Distributed Learning Service (ADLS), Military Personnel Data System (MilPDS), Defense Civilian Personnel Data System (DCPDS), and Automated Records Management System (ARMS).

In spite of the AF/A1 and AFDS efforts, AF IdM is currently stovepiped across various functional communities, where multiple instances of IdM capabilities are deployed by both independent organizations and applications. While the DAF has deployed "enterprise" identity solutions, like AFNet AD, even these tools fail to provide the full scope of access or authorization for a given identity. This leads each application or functional organization to purchase, deploy and maintain its own solution and implement a set of unique identities and access control lists (ACLs), eliminating any chance of an enterprise view of an individual identity. This duplication is inefficient, less effective, much more costly, and has an adverse effect on user experience.

2.2 Credential Management

Credential management is the set of practices which organizations use to issue, track, update, and revoke credentials for identities within their context.[6] These four stages constitute a lifecycle, which begins with binding an individual identity to an individually owned and controlled authenticator, during an approved validity period. As individual's identity attributes change over time, the sponsoring organization updates the credentials as needed. Once the individual leaves an organization, the sponsoring organization revokes the credential. Similar actions are applicable to NPE credentials, but neither the DoD, nor its Service Components, have developed and scaled a full NPE-identity lifecycle management process.

---

[5] The nine authoritative identity data stores are: Defense Civilian Personnel Data System (DCPDS); Exchange Contact Information Synchronization (ECIS) Stores; Information Assurance Officer Express (IAO Express); Military Personnel Data System (MilPDS); Manpower Programming and Execution System (MPES); Advanced Distributed Learning Service (ADLS); Defense Enrollment Eligibility Reporting System (DEERS); Enterprise Directory Services (EDS); and Global Directory Service (GDS).

[6] FICAM Architecture v3.1

DAF currently operates several authoritative DoD systems supporting the credential lifecycle, including the Defense Enrollment Eligibility Reporting System (DEERS) / Real-Time Automated Personnel Identification System (RAPIDS), PKI, and the Alternate Token Identity Management System (ATIMS). The DAF also operates PKI on behalf of DoD, to issue NPE credentials to domain controllers and workstations, for enabling smart card logon (SCL) and devices connected to DAF networks (DAF supports SIPR tokens and IC PKI certificates separately). However, the DAF is still limited to only a few DoD-approved authenticators, including the CAC, for issuing PE credentials. The CAC itself is not a suitable authenticator for all scenarios or environments, such as when using a mobile device to connect to DAF networks, services or data. While soft certificate-based solutions bridge part of this gap today, they still don't help those non-CAC holding individuals DAF must support.

2.3 Access Management

Access management controls how entities are granted or denied access to resources by combining authentication, authorization, and audit mechanisms.[7] DAF currently uses the DD Form 2875, System Authorization Access Request (SAAR), a manual, forms-based process, for all access requests. Multiple, independent efforts to automate this workflow process are ongoing and there is currently no policy requirement to use the 2875 form. However, the form itself continues to be the focus of these efforts, rather than realizing efficiencies through process automation.

Today, there are no DAF enterprise-wide access control mechanisms and local access control policies further fragment the access control landscape. Regardless of the control type (e.g., role-based or attribute-based), all DAF access controls are implemented local to the resource being accessed, making complete visibility into end-to-end user activity nearly impossible.

Authentication

Authentication is the process of verifying a claimed identity is genuine, based on valid credentials. DoD requires strong two-factor authentication (2FA) to deny or disrupt unauthorized access into DoD networks.[8] This requirement has driven DoD systems from relying on weaker username-password-based methods to using at least two of the three authentication factors: 1) something the user knows; 2) something the user has; and, 3) something the user is (physical characteristic). The most common 2FA in the DAF today, combines a personal identification number (something the user knows) and the PKI certificates on a CAC (something the user has). This has forced most DAF systems towards PKI-Enabled for 2FA compliant solutions. However, this limited solution fails to address any non-CAC holding users and user situation where the CAC is not the best 2FA form factor (e.g., mobile or development environments, shared user devices, biometric/automatic identification technology for physical access, etc.).

[7] FICAM Architecture v3.1
[8] DoD Cybersecurity Discipline Implementation Plan, Feb 16

Privileged Access Management (PAM)

Privileged users, such as system administrators, are assigned elevated access to protected resources, so they can perform security-relevant functions, which general users do not perform.[9] Because these functions can observe, execute, and maintain sensitive critical system operations, privileges must be constantly monitored for abuse and compromise. Without monitoring, this environment creates greater opportunities for misuse, insider threat activity and adversary compromise. Current PAM within the DAF is poorly implemented, largely relies on manual methods that are prone to error, do not consistently enforce the policy of least privilege, and often allow users unnecessary privileged access.

Authorization

Authorization enforces well-designed access policies to ensure the right entities are granted the right access to the right resources anytime, anywhere.[10] Data tagging, the process of associating relevant metadata information about data to the data itself, supports granular access controls, such as identity attributes, which in-turn improves authorization decision granularity. However, DAF Data tagging efforts are still largely in the exploratory stage, with the exception of our data from the IC, which received significant focus and funding to enable data sharing after 9/11, and our most forward leaning DevSecOps organizations. Today, AD is the DAF's primary authorization framework and current authorization capabilities depend on local access control lists. User authorization occurs as part of, or separately from, authentication and involves validating attributes associated with one or more roles. Currently, the DAF has no enterprise-wide authorization capability outside of the AD and Cloud-Hosted Enterprise System (CHES) environment. This forces users to complete separate authorization requests to each respective data owner; a process taking anywhere from a few hours, to several days for resolution.

2.4 Governance

An ICAM governance framework is a structure containing policy, guidance, standards, rulesets, and other directives to control how ICAM capabilities operate within a given system or enterprise. DAF currently implements an Enterprise IT (EIT) Management Framework, within which is a three-tiered governance structure consisting of a Group, Board, and Council bodies.

Today, the existing centralized governance framework is not sufficiently focused on DAF enterprise-level ICAM. Despite Air Force Instruction (AFI) 17-130 , Cybersecurity Program Management, highlighting ICAM as part of the Protect Cybersecurity Framework Core Function, existing DAF IT policy and its implementation (e.g., Air Force Policy Document (AFPD) 17-1, Information Dominance Governance and Management, etc.) has only addressed ICAM-related capabilities as part of an EIT program, rather than a major cybersecurity component. As a result, the DAF has no ICAM-specific policies[11] for adopting technologies to deploy enterprise-level ICAM capabilities.

[9] FICAM Privileged User Instruction and Implementation Guidance, v1.0, 15 Oct 14
[10] FICAM Roadmap and Implementation Guidance, v2.0, 2 Dec 11
[11] DAFMAN 17-1304, Identity, Credential and Access Management (ICAM), is still pending official publication

2.5 Federation

Federation is a set of processes and procedures for leveraging identity data and credentials that are managed outside of the DAF, such as other government agencies, coalition partners, industry and academia, to support authentication and authorization. It allows user populations to authenticate to their respective security enclaves and gain seamless access to other organizations' security enclaves, including other military services and intelligence agencies, as well as coalition, industry and academic partners. Current DAF identity federation and ICAM sharing capabilities are limited and only non-secure methods exist for authenticating and authorizing non-CAC holders. The DAF is only just beginning to address this significant shortcoming, via the Mission Partner Capabilities Office (MPCO). The MPCO defined Coalition PKI and federated identities as emerging capabilities that will contribute to improving DAF warfighter interoperability across the Mission Partner Environment (MPE), Battlefield Information Collection and Exploitation Systems (BICES), Combined Enterprise Regional Information Exchange (CENTRIX), and other relevant coalition networks.

3 Strategic Goals and Objectives

The goal state for DAF ICAM sets the foundation for Zero Trust Architecture and begins with a federated and centralized management process, creating fundamental trust in the digital identities of all person and NPEs interacting with DAF networks. It permits multiple approved authenticators, such as the CAC,FIDO2[12], hardware tokens, and mobile authenticators, which support various environments, users, devices, and missions. An industry standards-based enterprise ICAM user interface provides seamless, secure, and auditable access, consistent across classifications, automatically ensuring the right user has the right access to approved resources anytime, anywhere. It also includes automated application and enforcement of AF ICAM policies, guidance, and standards to evolve our cybersecurity into a more resilient defense posture. By adding enterprise federation, DAF creates trusted information exchanges across services, other government agencies, allies, and other key partners. DAF envisions a path to this goal state built on centralized identity management, universal authenticator support, seamless enterprise access management services, and a standardized DAF ICAM governance framework and policy enforcement.

3.1 Goal #1: Centralized Identity Management

Industry leaders agree that centralized identity management, as a single source of truth, is a foundational requirement for any successful identity strategy.[13] By implementing a single, distributed, scalable, extensible, and automated Identity as a Service (IDaaS) platform, which collates dynamic updates, DAF provides the trust necessary to support federated, enterprise-wide decision making. Therefore, DAF must establish a trustworthy process for assigning authoritative, normalized attributes from multiple sources to a digital identity and managing the lifecycle of each identity associated with a person or NPE. DAF also requires the ability to allow authorized mission partners secure access to its systems. Likewise, DAF users require the ability to securely access non-DAF systems for which they are authorized.[14] Together, these capabilities provide that foundational, single source of truth.

3.1.1 Objective #1.1: Establish Identity Attribute Data Policy

In order to centralize identity management, DAF must first define how to normalize and manage person and NPE identity data. Normalizing identity data requires a unique representation for all DAF identity attributes. By leveraging existing attributes and schemas, and using a standards-based process, normalized data enables sharing and aggregation from existing authoritative sources. DAF must also align, set and enforce data currency requirements to guarantee identity data remains synchronized both on and off premises, or in a disconnected environment. Finally, DAF must define and standardize NPE attributes and identify the DAFs trusted identity broker for NPE data. These are the foundational steps toward sharing identity data across the DAF and with federated identities across DoD and other mission and non-mission partners.

---

[12] FIDO2 is the umbrella term for a passwordless authentication open standard developed by the Fast Identity Online (FIDO) Alliance, an industry consortium comprised of technology firms and other service providers.
[13] Gartner, “Solution Criteria for Identity Governance and Administration,” 13 Dec 2019; Okta, “Identity Driven Security”; SailPoint, “SailPoint Solution Overview – Identity Credentialing and Access Management (ICAM/IdAM)”
[14] Air Force Identity Assurance Section (AFLCMC/HNCDI) Strategic Plan, Apr 2018

3.1.2 Objective #1.2: Implement a Single Identity Platform

DAF must provide a single organization and a single, virtual, distributed IdM platform into which all the stovepiped local ACL IdM solutions will transition (e.g., AFDS, AF/A1, SAP, etc.). DAF shall direct an effort to merge and normalize identity data from DAF active, guard and reserve – military, government, contractor – with data from retirees, dependents, and recruits into a repository within the single, virtual, distributed platform. The platform must collect, maintain and protect this data in accordance with stipulated laws, and regulations (e.g., System of Records Notice (SORN), Privacy Impact Assessment (PIA), etc.) to ensure DAF controls its own identities. It will also support disconnected and stand-alone networks at the same level of protection. Last, it must also present aggregated identity data to centralized internal and external authorization services accessible to all programs (e.g, commercial, cloud, AFNet, AFIN, and DoDIN partners) and across multiple network fabrics (e.g., NIPR, SIPR, SEC REL, etc) using cross domain solutions where necessary. DAF will not manage external identities but must support federation and interoperability with unanticipated users.

3.1.3 Objective #1.3: Automate Person Identity Lifecycle Management

DAF must normalize digital identities for the AFIN and properly retain from creation until the last surviving dependent passes away. Therefore, the centralized IdM platform must leverage existing authoritative identity data stores to support all lifecycle phases for person identities – creation; update (marital status, name, rank, duty location, retirement, separation, relocation, etc.); deactivation; and retention. In order to manage the massive amount of aggregated identity data from disparate authoritative sources, the IdM platform must automate this process and provide opportunities for individuals to manage their own identity attributes in a single, authoritative location. Together, this framework provides a trusted identity assertion to reliant systems, services, and applications.

3.1.4 Objective #1.4: Establish NPE Identity Lifecycle Management

DAF must establish an identity management lifecycle for NPEs similar to that already in place for PEs. This process must ensure only authorized NPEs are allowed access and resources are protected against intrusion and corruption by adversaries. DAF must align NPE identity attribute policy and standards with DoD to ensure emerging capabilities do not become stovepiped in the way person identities have. This includes deciding how to create and classify NPE identities (PKI/non-PKI), when to update, when to disable or delete and how long to retain NPE identities. This will also include automated processes for issuing, rotating, validating, and revoking credentials for DAF-issued, contractor provided and privately owned devices. DAF will also provide a method and means for authentication and identity management with disconnected AFIN NPEs (e.g., Industrial Control Systems). This provides a uniform approach to managing a set of devices that are quickly growing beyond control and better defines what we want from these devices.

3.1.5 Objective #1.5: Federate Identity Management with Mission and Non-Mission Partners

DAF will support the DoD ICAM Strategy goal of requiring credentials from mission and non-mission partners, who request access to protected resources, in order to promote responsible interoperability and data sharing.[15] DAF will collaborate with DoD and National Institute of Standards and Technology (NIST) to develop and maintain federated identity policy that provides risk-based guidelines to leverage acceptable external credentials to access AFIN resources and allow external agencies to accept DAF credentials.[16] The centralized IdM platform will serve as the DAF policy enforcement and decision points for vetting acceptable federated digital identities by implementing standard federation protocols (e.g., OpenID Connect (OIDC), WS-Federation, and Security Assertion Markup Language (SAML) 2.0). DAF will also develop a trust framework and work with mission partners to establish standards to support federated architecture.

3.2 Goal #2: Universal Authenticator Support

In order to deliver an improved user experience, which empowers Airmen, the DAF will allow multiple DoD-approved authenticators (e.g. hardware tokens and mobile authenticators) that support a wide range of users, devices, and mission and non-mission partners across a spectrum of mission environments and scenarios (e.g., airborne, terrestrial, etc.). The DAF will also deliver a public-facing, self-service, enterprise ICAM user interface where Airmen, retirees, dependents, and partners can map additional authenticators to their identity, reset passwords, and configure derived credentials. This interface will automatically approve and manage requests for alternate form factor authenticators at operationally relevant speeds.

3.2.1 Objective #2.1: Implement Operationally Effective Management Process for Alternate Form Factor Authenticators

In order to expand beyond CAC-based form factors, DAF must aggressively advocate for, validate, and authorize a variety of DoD-approved authenticators, supporting both CAC holders and non-CAC eligible personnel (e.g., retirees and dependents) and using industry-standard risk management guidance. DAF must evolve existing policy to define stakeholder roles and responsibilities, the request fulfillment path, and the lifecycle of an authenticator in this decision-making process. DAF will manage how requesting organizations collaborate with DoD to onboard newly approved authenticators into the centralized identity platform for use within the enterprise.

[15] DoD ICAM Strategy, 30 Mar 20
[16] Ibid

3.2.2 Objective #2.2: Deploy Enterprise Authenticator Interface

DAF must deploy a user interface supporting self-service authenticator management capabilities, such as: configuring derived credentials; assigning additional DoD-approved authenticators to themselves; and resetting the password credential(s) on their authenticator(s). The interface must also provide applications, services, and administrators' access to leverage authorized, available authenticators and identities. The enterprise ICAM user interface can also help users find which applications each authenticator supports and for which applications they are authorized access. This interface will be accessible to CAC and Non-CAC holding Airmen, retirees, dependents, partners and other members who fit more than one persona category, anytime, anywhere and from any Government Furnished Electronic (GFE) or DAF-approved personally owned device. The interface must also generate detailed logging information to existing detection tools, with sufficient context also sent to the requesting user, to confirm an action is not malicious. This reduces manual, labor-intensive provisioning, reducing costs and improving user experience.

3.2.3 Objective #2.3: Implement Single Management Process for Mission/Non-Mission Partner Authenticators

DAF must accept authenticators from external partners to facilitate effective resource sharing, in support of daily business and operational mission requirements. DAF must leverage the trust framework developed in Objective 1.5, as well as existing governing bodies and capabilities to create a standards-based policy for accepting and exchanging authenticators. It is critical our mission/non-mission partners agree upon these standards to meet a wide range of trust and capability levels. Ultimately, the decision-making and onboarding processes will integrate with the DAF management process for alternate form factor authenticators.

3.3 Goal #3: Seamless Enterprise Access Management Services

In order to save Airmen time, with faster access request responses, the DAF must evolve beyond existing manual, inconsistent, nonsecure access management processes, by balancing security and usability through centralized dynamic access mechanisms. DAF will implement centralized access management capabilities to automate account provisioning, de-provisioning, and privileged access management, reducing mission risk exposure. Concurrently, DAF will implement end-to-end (E2E) access management capabilities across mobile, cloud, and BYOAD, which leverage data tagging and allows authorized users lower-risk, on-demand access to resources anytime, anywhere.

3.3.1 Objective #3.1: Centralize Access Management Capabilities

DAF will centralize access management capabilities for authenticating and authorizing person and NPE access. This starts with a policy directing all system, application, and data owners to build or modify their rules governing access to their resources (including data tagging), based on trusted identity attributes and entitlements. The system will then leverage the most current tagged data and access rules, established by resource owners [as described by governance objective (4.3)], as input to the authorization decision making process. The resulting standardized access decision is qualified based on the associated authentication and authorization, as needed by the relying party. Together these capabilities simplify management and user's access to resources.

3.3.2 Objective #3.2: Automate Account Provisioning and De-Provisioning

DAF will transition away from the manual DD Form 2875, SAAR workflow process. This reduces administrator touchpoints by automating the workflow for account provisioning, de-provisioning, requesting resource access, and governing towards a fully automated process, based on a user's roles, attributes, and entitlements. As a user's attributes change (e.g., Permanent Change of Station (PCS), rank/grade, marital status, job assignment, security clearance eligibility, need-to-know, etc.) the system should assess the current identity configuration and provision or de-provision based on the new attributes. This process starts with implementing an enterprise Attribute-Based Access Control (ABAC) system and requiring system and application owners to leverage the centralized repository of resource access rulesets (defined in Obj 3.1). ABAC authorizations rely on evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships.[17] Users in ABAC, once provisioned, inherit the permissions defined for their assigned roles/group(s) and gain access to the roles'/group(s') authorized resources, such as shared network folders. Conversely, pre-defined conditions, such as individual users creating/archiving a Microsoft Teams channel, will automatically require and enforce continuous authentication or de-provision access decisions, without additional human interaction. While not every aspect can be automated, these measures improve overall access auditability and frees up users and administrators to focus on higher value tasks.

3.3.3 Objective #3.3: Automate Privileged Access Management

DAF must transition away from a manual process for PAM, towards one that is dynamic and limits persistent human privileged access as much as possible. A dynamic PAM will mitigate the risks associated with possible misuse, whether intentional or unintentional, and ensure proper oversight of these sensitive roles. It starts with a policy, which, at a minimum, enforces least privilege and segregation of duties, and defines appropriate privilege escalation conditions. DAF will then automate the privileged access lifecycle and enforce those policies using various approved commercial enterprise PAM solutions. The PAM solution will adjudicate privilege escalation and de-escalation based on pre-defined task and/or time constraints and specific system owner requirements (e.g., environment conditions, type of workstation/operating system, authentication method, etc.). By automating the privileged user management lifecycle, the DAF will ease the administrator burden to perform these manual actions, allowing them to focus on higher order cybersecurity activities.

3.3.4 Objective #3.4: Enable Authorized Data Access Anytime/Anywhere

Tomorrow's Air and Space professionals are expected to be as effective when operating in a disconnected, denied, degraded, intermittent or limited communication environment, as they are under normal operating conditions at their home station, leveraging the right devices and authenticators that best fits their given scenario. Therefore, DAF must prioritize the unique identity challenges and risks of employing mobile, cloud, and other remote or disconnected technologies, especially at OCONUS sites, providing a consistent user experience, regardless of environment.

[17] NIST SP 800-162, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", January 2014

Using the centralized access management and distributed infrastructure capabilities referenced in Objective 3.1 as the baseline, DAF must expand testing, policies, and systems to apply ZTA principles (e.g., user environment variables, system/device security posture), to a wide variety of inherently untrusted mobile devices. Strong partnerships with industry, to implement accredited Impact Level (IL) cloud environments (IL4 up to IL6), accessible OCONUS, will provide more secure, available and cost-effective worldwide access to resources. DAF must also develop the ICAM systems and associated policies, enabling disconnected and disrupted units to synchronize periodic snapshots of the centralized identity platform, to secure their standalone environments and provide edge authentication capabilities. Together, these capabilities modernize our digital Airmen's experience for warfighter effect.

3.3.5 Objective #3.5: Synchronize Data Tagging Implementation

The strength of DAF cybersecurity is growing more dependent on the quality, Visibility, Accessibility, Understandability, Linkages, Trustworthiness – Interoperability, and Security (VAULT-IS) of data as a strategic asset. For ICAM, the quality of authorization decisions depends on the quality and granularity of tagged data and data owner defined rulesets governing data access. SAF/CDO, as Chief Data Officer, is responsible for the DAF Data Implementation Plan of the DoD Data Strategy, inclusive of a data tagging policy. The DAF ICAM program is a key stakeholder and must establish a key relationship with SAF/CDO in this effort to best define the touchpoints to access required data.

3.4 Goal #4: Standardized DAF ICAM Governance Framework and Policy Enforcement

DAF cybersecurity relies on a strong ICAM governance foundation, providing the structure for programmatic oversight, as well as technical policy development and enforcement. Without all of these governance components, no one can know whom or what is accessing DAF networks, services or data at any time. Creating a centralized DAF ICAM governance body will provide a focal point to oversee and underwrite all aspects of the ICAM program. Adopting and automating enforcement of ICAM policies and standards provides a uniform security posture, minimizes risk potential, and realizes manpower savings across the enterprise. Continuously monitoring and auditing ICAM events, through AI mechanisms such as analytics and machine learning (ML), revolutionizes the DAF approach to cybersecurity for an agile and resilient defense posture. AI mechanisms, in turn, will also require monitoring to assure they perform as intended.

3.4.1 Objective #4.1: Create Centralized DAF ICAM Governance Body

The DAF must create a single, centralized body responsible for developing ICAM policies and guidance, to ensure uniform alignment and oversight, across the entire enterprise. Various network fabrics (e.g., JWICS, SAP, PIT, development networks, etc.) will require appropriate community stakeholder representation for their interests, beyond the traditional EIT governance structure. This governance also ensures a consistent approach to managing legacy identity and access services, converging existing stovepiped systems, as well as onboarding new ICAM acquisitions aligned with higher-level strategies.

Responsibilities of this body must include, but are not limited to:

- ensure all new acquisitions, implementation plans, and policy changes address legacy capability requirements;
- synchronize ICAM and EIT acquisition, implementation, and integration across the DAF and with external partners;
- serve as the focal point to ensure proper coordination, review, approval, and compliance of new and modified DAF, DoD, and other S/A ICAM governance policies; and
- sponsor early systems engineering efforts (ESE) to conduct ICAM risk assessments and prototype new capabilities.

3.4.2 Objective #4.2: Adopt Standards to Support ICAM Capabilities

In order to uniformly integrate ICAM across the enterprise, DAF must adopt a standards-based approach, which meets all functional requirements and mitigates against being locked into a single vendor, tool, or platform.

The DAF ICAM governance body must adopt and enforce industry standards and protocols to:

- integrate ICAM capabilities into the DAF enterprise architectures;
- leverage access management frameworks for authentication, authorization, and audit; and
- ensure uniform deployment, optimal use, flexible replacement, and sufficient oversight of approved ICAM technologies across the enterprise.

3.4.3 Objective #4.3: Automate ICAM Governance Enforcement

The effectiveness of any decision the governance body makes is completely dependent on the technical enforcement of those decisions. The sheer volume of near real-time information processed in these decisions requires an automated governance mechanism, aligned with any future DAF ZTA. This mechanism begins by accepting requests from users (PE or NPE), incorporating guidance from the policy repository and applying attributes about the user from a policy information point. With this information, any policy decision/enforcement point can now interrogate the mechanism to make decisions such as granting or denying access to resources, elevating privileges, delegating privileges, or stepping-up authentication. Based on industry standards, system owners can leverage multiple policy repositories, policy information points, and tagged data to form the basis of a tailored enforcement decision. This decision-making process is the heart of the centralized access management capability presented in Objective 3.1.

3.4.4 Objective #4.4: Monitor and Audit ICAM Events Through Analytics and Machine Learning (ML)

Continuous monitoring and auditing of ICAM events across DAF networks directly supports the need to drive out anonymity and increase awareness of entities seeking and gaining access to enterprise resources. DAF must automate enterprise-wide monitoring, auditing, and reporting of identity events for assurance that only authorized identities are able to gain access and utilize resources. The best analytics applies AI and ML techniques to large amounts of data gathered from multiple sources, analyzes the data to reveal both normal and anomalous behavior patterns, and guarantees currency and synchronization of identity data. ICAM audit and reporting will interface with existing network-level capabilities (e.g., Security Information Event Management (SIEM), Security Orchestration Automation and Response (SOAR), User and Event Behavior Analytics (UEBA)) to report additional anomalous and potentially malicious activity. It will also feed into a user's "identity risk score," helping to make automated access control decisions and allowing administrators to apply better-informed security pre-emption actions. The activity captured through this method also serves as input to ongoing audit and reporting processes, reducing labor-intensive review and analysis. However, within this process it is essential to retain human in the loop audit capabilities and competencies, which will leverage the power of automated analytics. Without a comprehensive audit and investigatory function, the DAF risks becoming overly dependent on complex automated systems, whose decision-making processes become indecipherable and effectively unreviewable.

4 Strategy Execution

The DAF is poised to provide its warfighters with the unparalleled and revolutionary advantages of a complete ICAM ecosystem and data-centric cybersecurity strategy. As Lead Command for Cyberspace Operations, Air Combat Command (ACC) is appointed to develop the DAF ICAM Implementation Plan, execute this Strategy, and synchronize all DAF ICAM developments informed by DoD ICAM efforts. Execution must include a time-phased implementation, which delivers an initial capability within 18 months and address all Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) considerations, capability prioritization, funding, sustainment, and describe the relationship with EIT and the EIT Management Framework. Due to the Zero Trust dependency on ICAM, as an overarching strategy, any DAF ICAM implementation must include close synchronization and alignment with Enterprise IT initiatives (including EITaaS, CloudOne, and Platform One), in order to maximize capability roll out and minimize project slippage. Implementation should begin with fixed NIPR/SIPR systems, apps and data first and extend to other network fabrics, tactical and operational missions and disconnected environments as progress matures. Any plans must include tasks and activities describing how existing legacy systems and capabilities will integrate with new ICAM policies and technologies. DAF proposes $143 million through FY27, at approximately $20 million per year, are required to implement this strategy. Ultimately, this strategy must evolve the current state of DAF ICAM into a more secure, efficient, and effective future state, which specifically enhances cybersecurity, interoperability, and end user access to and experience with enterprise services.

5 References

AFLCMC/HNCDI, "Air Force Identity Assurance Section Strategic Plan," Apr 18

DoD Cybersecurity Discipline Implementation Plan. (2016, Feb). [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

DoD ICAM Reference Design, v1.0. (2020, Jun). [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber

DoD ICAM Strategy. (2020, Mar 20). [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf

FICAM Architecture, v3.1. [Online]. Available: https://arch.idmanagement.gov/

FICAM Privileged User Instruction and Implementation Guidance, v1.0, 15 Oct 14

FICAM Roadmap & Implementation Guidance v2.0. (2011, Dec 2). [Online]. Available: https://playbooks.idmanagement.gov/assets/playbooks/Roadmap-FICAM-v2-20111202.pdf

Gartner, "Solution Criteria for Identity Governance and Administration," 13 Dec 19

NIST SP 800-63-3. "*Digital Identity Guidelines*." (2017, Dec 1). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

NIST SP 800-162. "*Guide to Attribute Based Access Control (ABAC) Definition and Considerations*." (2014, Jan). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

Okta, "Identity Driven Security"

OMB Memorandum M-19-17, "*Enabling Mission Delivery through Improved Identity, Credential, and Access Management*." (2019, May 21). [Online]. Available: https://whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

SailPoint, "SailPoint Solution Overview – Identity Credentialing and Access Management (ICAM/IdAM)"

This page intentionally left blank.

Appendix A Acronyms

2FA	Two Factor Authentication
ABAC	Attribute-Based Access Control
ACC	Air Combat Command
ACL	Access Control List
AD	Active Directory
ADLS	Advanced Distributed Learning System
AF	Air Force
AF/A1	Air Force Personnel Directorate
AFDS	Air Force Directory Services
AFI	Air Force Instruction
AFIN	Air Force Information Network
AFLCMC	Air Force Lifecycle Management Center
AFNet	Air Force Network
AFPD	Air Force Policy Directive
AI	Artificial Intelligence
ARMS	Automated Records Management System
ATIMS	Alternate Token Identity Management System
BICES	Battlefield Information Collection and Exploitation Systems
BYOAD	Bring Your Own Approved Device
CAC	Common Access Card
CENTRIX	Combined Enterprise Regional Information Exchange
CIO	Chief Information Officer
CO	Chief Data Office
CC/S/A	Combatant Commands / Services / Agencies
DAF	Department of the Air Force
DAFMAN	Department of the Air Force Manual
DCPDS	Defense Civilian Personnel Data System
DEERS	Defense Enrollment Eligibility Reporting System
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoDIN	DoD Information Networks
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and

	Education, Personnel, and Facilities
E2E	End-to-End
EDIPI	Electronic Data Interchange Personal Identifier
EIT	Enterprise Information Technology
EITaaS	Enterprise Information Technology as a Service
ESE	Early Systems Engineering
FICAM	Federal Identity, Credential, and Access Management
FIDO	Fast Identity Online
GFE	Government Furnished Equipment
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IDaaS	Identity as a Service
IdM	Identity Management
IL	Impact Level
IoT	Internet of Things
IT	Information Technology
JWICS	Joint Worldwide Intelligence Communications System
MilPDS	Military Personnel Data System
ML	Machine Learning
MPCO	Mission Partner Capabilities Office
MPE	Mission Partner Environment
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
OIDC	Open ID Connect
OMB	Office of Management and Budget
PAM	Privileged Access Management
PCS	Permanent Change of Station
PE	Person Entity
PIA	Privacy Impact Assessment
PIT	Platform Information Technology
PKI	Public Key Infrastructure
RAPIDS	Real-Time Automated Personnel Identification System
RPA	Robotic Process Automation
S/A	Service / Agency

SAAR	System Authorization Access Request
SAF	Secretary of the Air Force
SAML	Security Access Markup Language
SAP	Special Access Program
SCL	Smart Card Logon
SIEM	Security Information and Event Management
SIPRNet	Secure Internet Protocol Router Network
SOAR	Security Orchestration, Automation, and Response
SORN	System of Records Notice
UEBA	User and Entity Behavior Analytics
US	United States
VAULT-IS	Visibility, Accessibility, Understandability, Linkages, and Trustworthiness – Interoperable, SeVcure
ZT	Zero Trust
ZTA	Zero Trust Architecture