CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NOV 2 6 2024

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: DoD Identity, Credential, and Access Management Federation Framework

I am pleased to share the DoD Identity, Credential, and Access Management (ICAM) Federation Framework, a key milestone in our mission to enhance secure information sharing and interoperability across both internal DoD components and our trusted mission partners. This framework establishes a consistent approach to federating identity, credential, and access management (ICAM) systems, ensuring that trusted users from diverse organizations can securely access necessary information and applications.

The ICAM Federation Framework outlines a phased approach for implementing secure, scalable identity federation within the DoD and with external mission partners. Phase one addresses DoD-wide standardization of ICAM services to enable internal information sharing, while phase two builds connections with mission partners through trust agreements and aligned federation policies.

Integrating these federation practices into our ICAM systems will significantly advance our collective capability to operate securely and collaboratively in a complex threat landscape.

The points of contact for this matter are Mr. Robert W. Vietmeyer at (571) 372-4461, robert.w.vietmeyer.civ@mail.mil, and Mr. Tyler Harding at samuel.t.harding2.civ@mail.mil.

Leslie A. Beavers

Leslie A. Beavers
Acting

Attachment:
As stated

Department of Defense

Identity, Credential, and Access Management

Federation Framework

An essential component of ICAM to enable secure, reliable information sharing between DoD and its mission partners.

November 26, 2024

Version 1.0

Prepared by

DOD CIO Information Environment (IE)

Executive Summary

Ensuring U.S. national security depends on sharing information across all Department of Defense (DoD) Components[1], other U.S. Government departments and agencies, and non-U.S. Government mission partners and stakeholders. Sharing information across a diverse user population requires granting varied levels of access to users provisioned and credentialed by their own organizations that strongly validate their identities and mission needs. These users are provisioned with commonly understood attributes that define their qualifications and entitlements, which can be used to create an assertion or claim for the purpose of accessing information.

Identity federation is a term that spans policies, procedures, and technical capabilities necessary to ensure organizations can trust each other to share valuable information. Federation policy (FP) and procedures require established trust agreements describing how partner organizations operate their Identity, Credential, and Access Management (ICAM) systems judiciously, such that granting access to their personnel is safe. This *DoD ICAM Federation Framework* defines the DoD FP, process, and governance criteria.

There are two phases needed to establish federation that enable broader, secure sharing of information: internal and external. The first phase is to standardize and establish federation among the DoD-approved ICAM Service Providers operating the ICAM systems that will enable internal, DoD-wide information sharing. The operation of these DoD ICAM systems is documented in Federation Practice Statements to capture how the information sharing process is executed between internal DoD organizations.

The second phase is to establish connections between DoD and external mission partners. This involves comparing the two organizations' respective Federation Policies and supplemented by an ICAM Federation Trust Agreement between DoD and its external partner defining how their respective ICAM processes will interact.

To facilitate federation, the DoD Chief Information Officer (CIO) will establish a Federation Policy Management Working Group (FPMWG) under the existing ICAM governance structure to review ICAM federation documents and harness the institutional knowledge of ICAM subject matter experts.

This document describes the DoD federation policy, the elements that must be described in federation practice statements, and the foundational trust agreements that provide the building blocks to enable information sharing broadly. The resulting DoD Federation will enable a consistent, traceable, compliant, and secure, information-sharing environment capable of supporting a wide range of missions.

[1] The Office of the Secretary of Defense (OSD), the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

Contents

TABLES

1 Introduction

The DoD ICAM Federation is an essential component of DoD CIO strategy that aims to improve ICAM services and enable secure, automated, information sharing between internal and external partners across DoD. ICAM Federation establishes trust relationships that exchange Identity Provider (IdP) and/or ICAM Service Provider (SP) information between organizations to enhance information sharing. This framework establishes the DoD FP, which outlines the process for establishing ICAM federations within DoD and with external partners, and requires the creation, operation, and maintenance of an enterprise ICAM Federation Hub.

Federation allows an organization to accept ICAM information and decisions across organizational boundaries based on an established trust. For DoD's purposes, there are two types of Federated Trust: internal and external.

Internal federation is between DoD-approved ICAM SPs. Internal federation is established by ensuring each DoD organization's Federation Practice Statement (FPS) aligns to the DoD FP. Federation between approved ICAM SPs will ensure secure and interoperable access to systems and resources across the DoD enterprise, balancing the responsibility to share with the need to protect.

External federation is between DoD and organizations outside of DoD, commonly referred to as a mission partner, and is facilitated by mapping the external partner's FP to the DoD's FP and ensuring they are in alignment to aid in the development of an ICAM Federation Trust Agreement (IFTA). An IFTA is required between DoD and external federation partners because external organizations are not managed under the authority of DoD IT policy.

These agreements, policies, and practice statements will enable consistent, reliable, and secure communications while sharing between partners and across information domains. For instance, Mission Partner Environments (MPE) have a need to employ this federation across a wide range of internal and external partners. DoD CIO will adopt an ICAM Reference Architecture, revise the ICAM Strategy and Reference Design documents, and update other policy documents, as needed, to support successful implementation of federation.

2 Applicability and Scope

a. This document applies to:

   1. All DoD Components

2. All unclassified and classified DoD information systems (IS) and networks, including Special Access Program (SAP) information technology, under the authority of the Secretary of Defense.[1].
3. All DoD and non-DoD person entity (i.e., people) and Non-Person Entity (NPE) users accessing unclassified and Secret Fabric DoD information and information systems.
4. All DoD ICAM capabilities, functions, systems, elements, and services.
5. External organizations with whom the DoD CIO, as the DoD ICAM Federation Policy Management Authority (FPMA), has established an IFTA.

b. Nothing in this Framework alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of intelligence and intelligence-related information pursuant to Executive Orders 12333 and 13526 as well as other laws, regulations, and policies.

3 Framework Policy

a. DoD will pursue a coordinated and comprehensive federation capability to facilitate the efficient use of DoD resources and promote information sharing both within DoD and between DoD and its external mission partners to the maximum extent possible.

b. All DoD-approved ICAM SPs will maintain a current authorization to operate, comply with all requirements for ICAM SPs in section 4.3 of this Federation Framework, federate in accordance with the requirements in Section 5 of this Federation Framework (i.e., the DoD FP), and submit a FPS to the FPMWG that complies with the DoD FP.

c. All DoD ICAM Federations will be governed by this Framework. Internal DoD federation members (e.g., ICAM SPs) will operate under FPSs aligned to the DoD FP. External DoD federation members will adhere to the IFTAs established between the DoD and the external partner.

d. The DoD will evaluate and approve proposed internal and external federation members by assessing their ICAM and federation practices against the IdP requirements in section 3.6 of DoD Instruction (DODI) 8520.03, the Federation Assurance Levels (FAL) in National Institute of Standards and Technology (NIST) SP 800-63C, the DoD FP of this Federation Framework, and any other criteria necessary to determine if the federation is sufficiently secure for the data being shared.

e. Federations between Departments and Agencies on the U.S. Secret Fabric (to include SIPRNet) shall comply with this Framework and the appropriate Committee on National Security Systems (CNSS) issuances.

[1] e.g., Non-classified Internet Protocol Router Network [NIPRNet], Secret Internet Protocol Router Network [SIPRNet], Defense Research and Engineering Network [DREN], Secret Defense Research and Engineering Network [SDREN], SIPRNet Releasable [SIPR REL] De-Militarized Zone (DMZ), United States Battlefield Information Collection and Exploitation System [USBICES], and DoD Mission Partner Environment [MPE]

4 Roles and Responsibilities

This section identifies roles and responsibilities required to maintain secure ICAM transactions between federation members.

4.1 Federation Policy Management Authority (FPMA)

The DoD CIO is the DoD FPMA. The FPMA:

a. Serves as the DoD Federation Authority (FA) and establishes IFTAs with external DoD partners (e.g., federal, state and local, industry, or foreign partners).

b. Serves as the DoD approval authority for FP, IFTAs, and DoD Component or ICAM SP FPSs.

c. Directs and oversees the conduct of the FPMWG and delegates, as deemed necessary.

d. Establishes parameters regarding expected and acceptable security criteria for DoD federations with internal and external partners, such as the Identity, Authenticator, and Federation Assurance Levels in accordance with NIST SP 800-63.

e. Develops the Federation participant community, including expanding the community through considering agreements with other federations that share mutually supportive mission objectives.

f. Serves as arbiter for conflict resolution between DoD federation members and external partners.

4.2 Federation Operator/Manager

The DoD Defense Information Systems Agency (DISA) is designated as the DoD ICAM Federation Operator/Manager (FO/FM). The FO/FM:

a. Establishes, operates, manages, and maintains the DoD ICAM federation hub. The Federation Hub shall have, at a minimum, the capability to:

   1. Register federation members.
   2. Establish and maintain discovery functions.
   3. Provides a mechanism to restrict the operations of specific Federation members in the event of a cybersecurity incident in the member network.

b. Validates and monitors federation membership to ensure compliance with FP.

c. Deliver and standardize Application Programming Interfaces (API) and protocols to ensure interoperability among federation partners.

d. Provide a uniform interface (i.e., a dashboard) to share attack and compromise information in real-time.

e. Collect and distribute analytical data among the federation members and the FPMWG.

f. Post FPSs and IFTAs approved by the FPMA on a DoD Federation website.

4.3 Approved DoD ICAM Service Providers

The DoD-approved ICAM SPs:

a. Serve as the initial DoD internal federation members.

b. Assign a voting representative to the FPMWG.

c. Document the practices, procedures, and processes to manage and maintain their ICAM services in a DoD Federation Practice Statement (FPS) in accordance with the FPS template in Attachment A.

d. Submit their approved FPS to the FPMWG for review and FPMA approval.

e. Assess and audit their home IdP (i.e., their own IdP) operations on an annual basis, and submit results to the FPMWG within 30 days of the audit's completion.

f. Ensure the minimum identity attributes identified in their FPS are included in any assertions issued by their home IdP.

g. Ensure additional identity attributes are available upon valid request of a Relying Party (RP) and provided by their home IdP to the RP.

h. Provide written notice to the FPMA, no less than 30 days prior to planned changes in their IdP assertions. If operational issues or security concerns require a Federation member to take immediate action, notice shall be provided to the FPMA within 1 hour.

i. Designate a Federation POC to report compliance and operational status of Federation capabilities, and to represent the DoD ICAM SP at the FPMWG.

j. Employ appropriately tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard for all Federation capabilities.

k. Support contested, degraded, or operationally limited environments and provide details on this support in their FPS.

4.4 DoD Federation Policy Management Working Group

The FPMWG is an action officer-level working group, under the authority, direction, and control of the FPMA. The DoD CIO, Director of Capability Oversight (CO), serves as the chairperson for the FPMWG. The FPMWG:

a. Serves as the initial governance forum for DoD components and Federation partners, to introduce nominees for Federation and examine DoD FP change requests (CR).

b. Reviews, manages, and audits Federation documentation.

c. Reviews CRs to the DoD FP and provide recommendations to the FPMA regarding CR approval.

d. Reviews new FPSs, evaluate their compliance with the DoD FP, and provide recommendations regarding their approval to the FPMA.

e. Reviews proposed changes to approved FPSs and votes on whether the Chair should approval.

f. Periodically assesses approved FPSs of DoD ISPs, and ensure they comply with the DoD FP.

g. Ensure both internal and external federation members submit an annual self-assessment and audit of IdP operations to the FPMWG, and approve these assessments and audits based on the recommendation of the FPMWG.

h. Review written notices provided by internal and external federation members regarding planned changes to their IdP assertions.

i. Ensure the IdP assertions of DoD internal Federation members support the minimum identity attributes identified in their FPS.

j. Ensure DoD external federation members’ FPs continue to align with the DoD FP via periodic re-mapping of each-other’s FPs after major FP updates, additional interoperability testing when DoD or the external partner makes changes or additions to its ICAM services, and periodic review of IFTAs.

k. Receive and review the annual audits of IdP operations submitted by DoD internal and external federation members and recommend approval or disapproval to the FPMA. The FPMWG will maintain records of the federation member audits for a minimum of five years.

g. If a DoD RP needs additional attributes for access management decisions, coordinate with the appropriate DoD internal federation members to ensure support.

l. Draft an FPMWG charter with further details on FPMWG membership, processes, procedures, and operations for signature by the FPMA.

4.5 DoD Components

DoD Components shall:

a. Provide representatives to participate in the FPMWG and other DoD ICAM Federation bodies as may be established in support of this Framework.

b. Identify eligible external organizations and their trusted officers to join the DoD Federation and refer them to the FPMWG for evaluation of their FP.

c. In the event of a unique and urgent mission critical need, seek approval from their DoD Component chief information security officer and the FPMA to establish a bilateral trust agreement and federation with an internal or external federation partner outside of the DoD Federation. The DoD FPMA must be notified in writing, with risks identified and mitigations documented in both the notice and the DoD Component's FPS (if applicable). The FPMA shall have final approval authority.

4.6 DoD External Federation Partners

DoD external partners will do the following to become and remain DoD external federation members:

a. Establish a IFTA with the FPMA and operate in accordance with that agreement.

b. Operate their home IdP in accordance with the standards documented in the IFTA.

c. Successfully complete yearly self-assessments and audits of the IdP operations.

d. Ensure the minimum identity attributes identified in their IFTA are included in any assertions issued by their home IdPs.

e. Ensure additional identity attributes are available upon valid request from a DoD RP via their home IdP.

f. Give written notice no less than 30 days prior to planned changes in the Federation member IdP assertions or change in status of any DoD-approved federation member to the DoD FPMA. If operational issues or security concerns require the Federation member to take immediate action, notice shall be provided within 24 hours.

g. Notify the DoD FPMWG, in writing, of the successful completion of their annual audit and provide the results of the audit upon request.

h. Designate a Federation POC for their organization to maintain compliance and operational status of Federation capabilities, and to communicate with DoD on federation-related matters.

i. Employ appropriately tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard for all Federation capabilities.

5 Federation Policy

This section outlines the DoD Federation Policy. The following are the technical requirements supporting federation.

5.1 Identity Provider Technical Requirements

An IdP is a system that performs direct authentication of entities based on their credentials and issues assertions derived from those credentials. Assertions may contain attribute information in addition to identity information. The DoD Federation will have internal IdPs operated by Approved ICAM Providers and external IdPs operated by external Federation members who join the DoD Federation. The following is a list of requirements for IdPs:

a. Perform authentication for end users/subscribers.
b. Only allow DoD-approved methods of authentication.
c. Provide minimum required person and non-person entity identity attributes.
d. Generate assertions containing the following metadata:
   1. Subject: Identifier for the party the assertion is about
   2. Issuer: IdP Identifier issuing the assertion
   3. Audience: Identifier for RP (assertion consumer)
   4. Issuance: assertion timestamp
   5. Expiration: time assertion expires and should no longer be accepted by RP
   6. Identifier: Value uniquely identifying the assertion
   7. Signature: Digital signature of assertion including public key of IdP (for certificate-based authentication)
   8. Authentication: Timestamp when IdP verified presence of subscriber at the IdP through a primary authentication event.
   9. Attribute metadata (see NIST Interagency or Internal Reports (NISTIR) 8112)

10. NIST SP 800-63A Identity Assurance Level (IAL) when identity proofed attributes are being asserted.
11. NIST SP 800-63B Authenticator Assurance Level (AAL) when an authentication event is being asserted.
12. NIST SP 800-63C Federation Assurance Level (FAL) of the assertion.

e. Disclose attributes through a data identity API rather than through the assertion itself.

f. Each federation member will register the home IdP metadata with a Metadata Registration service provided by the Federation Operator. IdPs will register the following metadata at a minimum:
   - Role Descriptor.
   - Entity ID.
   - Affiliation Descriptor.
   - Contact Person.
   - Organization URL.

g. When establishing a federation, the IdP shall disclose the details required to make a request to the RP or federation partner:
   - The list of attributes provided.
   - The possible range of IAL, AAL, and FAL supported by the IdP.

5.2 Minimum Required Entity Identity Attributes

Attributes allow the right entity to obtain the right information from a participating relying party. Attributes will be detailed in the Trust Agreements.

5.3 Reauthentication and Session Requirements

In a federated environment, the RP manages its sessions separately from any sessions at the IdP. The session at the RP starts when the RP processes the federation protocol from the IdP. At the time of a federated login, the subscriber may have an existing session at the IdP, which may be used as part of the authentication process to the RP. The IdP shall communicate any information it has regarding the time of the latest authentication event at the IdP, and the RP may use this information in determining its access policies. Depending on the capabilities of the federation protocol in use, the IdP should allow the RP to request that the subscriber re-authenticate at the IdP as part of a federation request.

The subscriber is capable of terminating sessions with the IdP and RP independently of one another. The RP will not assume that the subscriber has an active session at the IdP past the establishment of the federated log in. The IdP will not assume that termination of the subscriber's session at the IdP will propagate to any sessions that subscriber would have at downstream RPs.

5.4 Establishing Federation Entity Identities (ID)

A Federation Entity Identity (ID) is a globally unique name for a Federation entity, i.e., your IdP or SP. It is how other services identify your entity. Like any other unique identifiers, you share to interoperate with others, making sure your identifier is clear, unique, and permanent is critical for successful continued operation of your service(s).

Make every effort to choose an ID that will persist indefinitely. Services that interoperate with you, use your ID to look up your metadata. Changing an ID once your service (IdP or SP) is in operation leads to complicated change management efforts across all federation members.

Tips for creating a clear, meaningful ID:

- An ID SHOULD be an absolute URL starting with “https://”
- The URL SHOULD NOT contain a port number, a query string, or a fragment identifier
- The host part of the URL SHOULD NOT contain the substring “www”
- The URL SHOULD NOT end with a slash (/)
- An ID SHOULD NOT be more than 30 characters in length
- Include the substring "idp" in an IdP ID
- Include the substring "sp" in an SP ID

Additional notes: An ID is a name. It need not be a resolvable web location. SAML entity IDs must be a Universal Resource Identifier (URI). An ID is a persistent identifier, not a web location. An ID need not resolve to an actual web resource.

Examples of IDs

IdP names:

- https://USA_DoD.mil/idp_01
- https://USA_NAVY.mil/idp01
- https://UK_MOD.gov.uk/idp01

SP names:

- https://USA_DoD_comanage.example.mil/sp
- https://wiki.cs.example.org/sp

5.5 Auditing and Continuous Monitoring Requirements

IdPs of internal DoD-approved ICAM Service Providers and external member IdPs, will be audited upon joining the Federation. In the initial process of completing the Federation Practice Statement or a Federation Trust Agreement, the applying member will conduct a self-assessment using the auditing criteria in section 2.1 of the Federation Practice Statement.

Upon successfully completing the self-assessment, the FPMA will identify an approved third-party assessor to complete an independent audit in accordance with NISTIR 8149 “Developing Trust Frameworks to Support Identity Federations”. This audit must be reviewed on an annual basis, whenever there is a significant change in the operation of the IdP or an observed incident resulting in a significant loss.

Audit log files will be generated and stored in a tamper-evident manner for all events relating to the security of the IdP. All security audit logs, both electronic and non-electronic, will be retained and made available during compliance audits.

Components should follow standard cybersecurity guidance with respect to logging and audits. For example, DoDI 8520.03 includes the following requirements for IdPs: 4(d) Be audited at least annually to verify that operation is in accordance with the IdP's documentation 4(m) Log all authentication requests and maintain logs sufficient to support review of logs for evidence of fraudulent activity. Other existing DoD Cybersecurity policies set the standards for how long audit logs need to be retained. There is an expectation that IdPs will follow these DoD policies. Nothing in this policy relieves DoD Components or Members of the Federation of the need to perform auditing and logging in compliance with existing policy.

5.5.1 Types of Events Recorded

Security auditing capabilities of IdP and FO operating system and applications will be enabled during installation and initial configuration. At a minimum, each audit record will include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred.
- Success or failure where appropriate, and
- The identity of the entity and/or operator that caused the event.
- Time shall be synchronized with an authoritative time source to within three minutes.
- A message from any source requesting an action by the IdP or FO is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents. Where events cannot be electronically logged, the IdP and FO shall supplement electronic audit logs with physical logs as necessary.
- Other activities to be monitored will include:
    - Authentication transactions
    - Access of resources at a relying party
    - Additional attribute request transactions from the relying party to validate entitlements
    - End-to-end Transaction encryption

NOTE: Use DoD minimum requirements detailed in the FPS and Zero Trust monitoring and auditing minimum capabilities

5.5.2 Continuous Monitoring for Authentication and Access

Identity federation is a framework of trust between parties for the purpose of validating user identity, issuing user authentication claims or assertions and conveying information as attributes that would be needed to authorize access to resources. Participating organizations are unrelated except for specific Federation entity agreements for accessing the requested data or resources. In this context, there is a need to have a continuous monitoring capability that can track authentication and access transactions from multiple IdPs and federation SPs. Continuous monitoring reports will be submitted to the Federation Policy Management Working Group quarterly. Guidance for continuous monitoring can be found in NIST 800-137.

6 Federation Agreements

6.1 Agreements with a Single External Partner

Comply with this ICAM Federation Framework and use the template at Appendix B. May be considered a Bilateral agreement.

6.2 Trust Agreements between DoD and other External Federations

If it becomes necessary to establish a single federation with multiple external partners, DoD will seek to negotiate a trust framework in addition to bilateral IFTAs. A trust framework is the set of rules and policies that govern how the federation members will operate and interact. The trust framework will serve as the basis for any multilateral agreements and will help enable the trust and governance of a federation’s operations among the Federation members. The trust framework rules and policies will include, but not be limited to, how members will:

a. Conduct identity management responsibilities.
b. Share identity information.
c. Use identity information that has been shared with them.
d. Protect and secure identity information.
e. Perform specific roles within the federation; and
f. Managing liability and legal issues.

7 Federation Framework References

DoD Directive 5144.02, “DoD Chief Information Officer (DoD CIO),” November 21, 2014, as amended

DoD Instruction 5200.48, “Controlled Unclassified Information (CUI),” March 6, 2020

DoD Instruction 5230.09, “Clearance of DoD Information for Public Release,” January 25, 2019, as amended

DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” May 18, 2023

DoD Instruction 8520.03, “Identity Authentication for Information Systems,” May 19, 2023

Office of the Chief Information Officer of the Department of Defense, “DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design,” June 2020

Office of the Chief Information Officer of the Department of Defense, “DoD Zero Trust Reference Architecture,” July 2022

Identity, Credential, Management and Access (ICAM) Strategy, March 30, 2020

Department of Defense (DoD) Zero Trust Reference Architecture, v2.0, July 2022

DoD Zero Trust Strategy, October 21, 2022

NIST Special Publication NIST SP 800-217 initial public draft, Guidelines for Personal Identity Verification (PIV) Federation, January 2023

NIST Special Publication 800-63-A, B, C, 3, Digital Identity Guidelines, June 2017

8 Federation Framework Acronyms

Table 1. Acronyms

Acronym	Meaning
AAL	Authentication Assurance Level
ABAC	Attribute Based Access Control
COI	Community of Interest
CDO-L	Contested, Degraded, or Operationally Limited
CUI	Controlled Unclassified Information
DoD	Department of Defense
EDIPI	Electronic Data Interchange Person Identifier
FAL	Federation Assurance Level
FA	Federation Authority
FO	Federation Operator or Manager
FPMWG	Federation Policy Management Working Group
FPS	Federation Practice Statement
IA	Information Assurance
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
IdP	Identity Provider
IFTA	ICAM Federation Trust Agreement
MFA	Multi-Factor Authentication
ARRANGEMENT/AGREEMENT	Memorandum of Agreement
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RP	Relying Party
RD	Reference Design
ZT	Zero Trust

9 Federation Framework Glossary of Terms

The terms used in this DoD ICAM RD remain consistent with ICAM-related language in other documents and architectures, particularly FICAM architecture. Table 3 provides a glossary of terms used within this Framework.

Table 2. Glossary

Term	Description
Access Management	The set of practices that enables only those permitted the ability to perform an action on a particular resource. *--FICAM Architecture*
Assertion	A statement from a verifier to a Relying Party (RP) that contains information about a subscriber. Assertions also may contain verified attributes. *--NIST 800-63-3*
Assurance Level	The grounds for confidence that the set of intended security are effective in their application. *-- CNSSI 4009*
Attribute	A quality or characteristic ascribed to someone or something. *-- NIST SP 800-63*
Attribute Based Access Control (ABAC)	An access control paradigm whereby access rights are granted to users through policies which combine attributes together. The policies can use any type of attributes. (Also see Role Based Access Control) *-- NIST CSRC Glossary*
Attribute Service	A data repository where authorization attributes are collected and managed for a set of entities that is recognized as having the authority to verify the association of attributes to an identity, accessible only through a service that both provisions and serves up authorization attributes.
Authentication	The process by which a claimed identity is confirmed, generally through use of a credential. --FICAM Architecture

Term	Description
Authenticator	Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity -- *NIST SP 800-63*
Authenticator Assurance Level (AAL)	A category describing the strength of the authentication process. -- *NIST SP 800-63*
Authoritative Attribute Source	A data repository where authorization attributes are on-boarded and managed for a set of entities.
Authorization	The process by which a request to perform an action on a resource is decided, typically based on a policy. (Also see Access Management) -- *FICAM Architecture*
Authorization Attribute	An attribute used in authorization decisions.
Community of Interest (COI)	A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes. -- *NIST CSRC Glossary*
Contested, Degraded, or Operationally Limited (CDO-L)	*Contested operations are defined by degradation caused by enemy action, Degraded system operations are defined by degradation caused by failed systems or battle damage, Operational limitations are defined by reduced mission effectiveness caused by the physical or operational environment – Views November–December 2014 Air & Space Power Journal | 130SCHRIEVER ESSAY WINNER THIRD PLACE* *"Space Resilience and the Contested, Degraded, and Operationally Limited Environment"*

Term	Description
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. While common usage often assumes that the subscriber maintains the credential, these guidelines also use the term to refer to electronic records maintained by the CSP that establish binding between the subscriber's authenticator(s) and identity. *-- NIST SP 800-63*
Credential Management	The set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context. *--FICAM Architecture*
Digital Policy Rule	A rule that defines the combination of attributes under which an access may take place *-- CNSSI 4009 ABAC*
Entitlement	Authorization to access one or more resources within an information system
Entitlement Provisioning Service	A data repository that stores entitlements for a set of entities, provides an interface for managing those entitlements, and provides entitlements to information systems. This repository is accessible only through the service that both provisions and serves up entitlements.
Entity	A person, role, organization, device, or process that requests access to and uses resources.
Federated Entity	An entity whose identity is managed external to the DoD enterprise but who possesses a credential and potentially attributes managed external to the DoD that are approved for use within the DoD.
Federation	The ability of one organization to accept another organization's work. Federation is based on inter-organizational trust. The trusting organization must be confident that the trusted organization has similar policies, and that those policies are being followed. *-- FICAM Architecture*
Federation Authority (FA)	Senior individual to manage and oversee the DoD ICAM Federation.

Term	Description
Federation Assurance Level (FAL)	A category describing the assertion protocol used by a federation to communicate authentication and attribute information (if applicable) to a relying party. *-- NIST SP 800-63*
Identifier	Unique attribute that can be used to locate a specific identity within its context *--FICAM Architecture*
Identity	The set of characteristics (also called “attributes”) that describe an entity within a given context. (Also see Digital Identity) *--FICAM Architecture*
Identity Assurance Level (IAL)	The degree of confidence that the applicant’s claimed identity is their real identity. *-- NIST SP 800-63*
Identity Credential and Access Management (ICAM)	The set of security disciplines that allows an organization to enable the right entity to access the right resource at the right time for the right reason. It is the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. These resources may be electronic files, computer systems, or physical resources such as server rooms and buildings. *--FICAM Architecture*
Identity Provider (IdP)	A system that performs direct authentication of entities based on their credentials and issues assertions derived from those credentials. Assertions may contain attribute information in addition to identity information. *-- DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design*
Log Management System	A data repository that hosts ICAM related event logs.
Master User Record (MUR)	A data repository that hosts a record of all entitlements entities have been granted.

Term	Description
Mission Member	An organization with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; State and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. -- *DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design*
Mission Partner Entity	A person entity or NPE who is a member of a DoD mission partner
Multi-Factor Authentication (MFA)	A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. -- *NIST SP 800-63*
Non-Person Entity (NPE)	A physical device, virtual machine, system, service, or process that is assigned an identifier and may be issued credentials to support authentication and authorization.
Person Entity	An individual acting as themselves or in the capacity of a role that is assigned an identifier, assigned attributes, issued credentials, and provided with entitlements to support authentication and authorization.
Policy Decision Point (PDP)	Mechanism that examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration. -- *NIST CSRC Glossary*
Policy Enforcement Point (PEP)	A system entity that requests and subsequently enforces authorization decisions. -- *NIST CSRC Glossary*

Term	Description
Provisioning	Linking and unlinking access permissions for a person or entity to a protected resource. -- *FICAM Architecture*
Relying Party (RP)	An entity that relies upon the subscriber’s authenticator(s) and credentials or a verifier’s assertion of a claimant’s identity, typically to process a transaction or grant access to information or a system. (Also see Information System) – *NIST SP 800-63*
Requestor	An entity requesting that another entity be authorized access to a resource. The requestor may be the entity that is requesting access or may be another person or NPE requesting the access on the entity’s behalf.
Resource Attribute	Attribute applied to a resource rather than to an entity.
Resource Policy Service	A data repository where digital policy rules governing access to resources are stored.
Reviewer	A person or NPE responsible for reviewing ICAM related logs.
Role	A job function or employment position to which person entities or other system entities may be assigned in a system. -- *NIST CSRC Glossary*
Role Based Access Control (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. (Also see Attribute Based Access Control) -- *NIST CSRC Glossary*
Service Provider (SP)	A service provider is a federation resource that provides services to the end user. Typically, SPs do not authenticate users but instead request authentication decisions from an identity provider.
Transaction	A discrete event between user and systems that supports a business or programmatic purpose.
Zero Trust (ZT)	Zero Trust is an IT security model that requires strict identity verification for every person and device trying to access resources on a network, regardless of whether they are accessing from within or outside of the network perimeter.

Appendix A: Federation Practice Statement Template

Replace with your ORG Logo

Department of Defense or DoD Component Identity, Credential, and Access Management Federation Practice Statement

Version x.xx

Month Day, Year

The following Federation Practice Statement (FPS) template provides a basic model for a Department of Defense (DoD) FPS written to comply with the requirements in the DoD federation policy (see section 5 of the Identity, Credential, and Access Management (ICAM) Federation Framework dated August 13, 2024 (Federation Framework)). It is important to tailor the FPS to the specific needs and context of the organization implementing it. FPSs may contain additional details about the operations of the organization's federation but must provide the minimum information laid out below.

Federation Practice Statement

1. Introduction

- Purpose of federation

- Scope of federation

2. ICAM Operations

- Describe ICAM operations, to include technical details, design, and architectural viewpoints.

- Describe how Identity Assurance Level IAL,Authentication Assurance Level (AAL), and access requirements align with information sensitivity.

- Describe the Risk Management Framework (RMF) Confidentiality Impact level of the systems & other services using the IdP.

2. IdP Technical Requirements

- Describe compliance with section 5.1 of the Federation Framework.

- Describe alignment with the Identity Provider (IdP) requirements in section 3.6 of DoD Instruction 8520.03.

- Describe and provide justification for the National Institute of Standards and Technology (NIST) SP 800-63C Federation assurance level (FAL) of the IdPs assertions.

3. Entity Identity Attributes

- Describe compliance with section 5.2 of the Federation Framework, including technical and architecture details.

4. Reauthentication and Session Requirements

- Describe compliance with section 5.3 of the Federation Framework.

5. Federation Entity Identity Requirements

- Describe compliance with section 5.4 of the Federation Framework.

6. Auditing and Continuous Monitoring Requirements

- Describe compliance with section 5.5 of the Federation Framework.

7. Additional Practices

- Describe process for evaluating new ICAM or federation capabilities or modifications.

- Describe any relevant ICAM or federation practices not previously covered.

8. Conclusion

- Contact information for further inquiries.

Appendix B: Federation Trust Arrangement/Agreement

BETWEEN

THE UNITES STATES DEPARTMENT OF DEFENSE

FEDERATION MANAGEMENT AUTHORITY

AND

[External Organization]

WHEREAS [organization] and the United States Department of Defense (DoD) Identity Credential and Access Management (ICAM) Federation Authority (FA) desire to establish a trust relationship between their Identity Providers (IdP) in support of establishing an identity federation to allow each organization's personnel to access the other's network resources.

WHEREAS the DoD ICAM FA recognizes the need for non-DoD entities and personnel to interoperate with DoD relying parties for the purpose of conducting business electronically with the DoD.

NOW, THEREFORE, THE PARTIES HEREBY AGREE AS FOLLOWS:

1.0 Purpose.

This Trust Arrangement/Agreement describes the terms and conditions by which assertions issued by the federation member's "home" IdP are to be used to interact with DoD relying parties and access data authorized to be released in accordance with DoD policies and regulations. The federation member shall operate an IdP defined by a Federation Policy (FP) or Federation Practice Statement (FPS) governing the Federation member's operation.

2.0 References.

a. National Institute of Standards and Technology (NIST) Special Publication 800-63A-C, Digital Identities Guidelines.

b. NIST Special Publication 800-217, Guidelines for Personal Identity Verification (PIV) Federation.

c. DoD Directive 8520.03 Identity, Credential and Access Management for the Department of Defense.

d. DoD Identity, Credential and Access Management Reference Design, v1.0, July 20, 2020.

e. DoD Identity, Credential and Access Management Federation Framework, Draft.

f. OMB Memorandum, M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management.

g. DoD Enterprise Identity Attribute Service (EIAS) Person Entity Attribute Data Set Standard, April 1, 2022.

3.0 Authority.

The Electronic Signatures in Global and National Commerce Act (Public Law 106-229—June 30, 2000, codified at 15 U.S. Code Section 7000 et seq.) and the Government Paperwork Elimination Act (Title XVII of Public Law 105-277—October 21, 1998, codified at 44 U.S. Code Section 3504).

4.0 Background.

This ARRANGEMENT/AGREEMENT establishes an identity trust relationship between DoD and [external organization] to support authentication and authorization to each other's network resources.

In accordance with the procedure set forth in reference (e) of this arrangement/agreement, the DoD FA and the Federation member, as signatories to this arrangement/agreement, intend to maintain a trust path between their respective IDPs, as outlined herein.

5.0 Responsibilities.

a. By signing this arrangement/agreement, the Federation member shall:

i. Comply with the NIST requirements to issue and maintain credentials at Identity Assurance Level [1/2/3] in accordance with its Federation Practice statement.

ii. Operate the home IdP in accordance with the agreed standards in Annex A.

iii. Successfully complete yearly self-assessments and audits of the IdP operations.

iv. Ensure the identified minimum identity attributes (Annex B) are included in all assertions issued by the home IdP/s.

v. Ensure that additional identity attributes (Annex B) are available upon valid request of a relying party and relayed by the DoD home IdP.

vi. Give written notice via email to the Federation Operator and the FA no less than 30 days prior to planned changes in the Federation member IDP assertions or change in status of any DoD-approved federation member to the DoD FA. If operational issues or security concerns require the Federation member to take immediate action, notice shall be provided at the earliest opportunity and, in any event, within ten days by email to [email address].

vii. Notify the DoD FA immediately when a cybersecurity incident has occurred on *{Country}* network and when the incident has been resolved.

viii. Notify the DoD FA that its annual audit has been completed, within 30 days of its completion. The DoD FA may request confirmation of the successful completion of the audit, or the results of the audit itself, from the Federation member.

b. By signing this arrangement/agreement, the DoD FA shall:

i. Operate the home IdP in accordance with the agreed standards in its Federation Policy or Federation Practice Statement

ii. Successfully complete yearly self-assessments and audits of the IdP operations.

iii. Ensure the identified minimum identity attributes are included in any assertions issued by the home IdP/s.

iv. Ensure additional identity attributes needed for access management decisions are available upon valid request of a relying party and relayed by the DoD home IdP.

v. Provide written notice no less than 30 days prior to planned changes in the DoD IDP assertions, or change in status to federation member/s. If operational issues or security concerns require DoD to take immediate action, notice shall be provided at the earliest opportunity and, in any event, within ten days by email to [email address].

vi. Notify the federation member/s that its annual audit has been completed, within 30 days of its completion. The DoD FA may confirm the successful completion of the audit, or the results of the audit itself.

vii. Notify the federation partner immediately when a cybersecurity incident has occurred on the DoD network and when the incident has been resolved.

By posting changes or a new version of the FP/FPS, give written notice of changes in the DoD federation architecture or change in status within the DoD IDP to the Federation member no less than thirty (30) days prior to the changes being implemented. Notice of such changes will also be posted on the Cyber web site (https://cyber.mil/ICAM).

6.0 Agreements.

a. This arrangement/agreement is enforceable only by the parties and is binding upon the parties, by and through their officials, agents, and employees. No person or entity is intended to be a third-party beneficiary of the provisions of this arrangement/agreement for purposes of any civil, criminal, or administrative action, and accordingly, no person or entity may assert any claim or right as a beneficiary or protected class under this arrangement/agreement in any civil, criminal, or administrative action. Similarly, this arrangement/agreement does not authorize, nor shall it be construed to authorize, access to any documents by persons or entities not a party to this arrangement/agreement.

b. The Federation member understands that neither DoD nor the Federal Government will compensate it for the operation of its IDP.

7.0 Termination for Cause.

This arrangement/agreement may be terminated for cause by the DoD FA. Should the Federation member not comply with its obligations under its FP/FPS, should the Federation member fail an audit, or should the DoD FA become aware of any other issue that places the security of the Federation member in question, DoD FA may remove the Federation member. Justification for such action includes material violations of this arrangement/agreement or the Federation member's FP/FPS, such as intentionally failing to comply with the Responsibilities listed in Section 5 of this document. The written notification will be provided and include the reason(s) for the removal of the Federation member IdP from the federation manager approval list and provide the Federation member with sixty (60) calendar days to remediate any alleged violation or non-compliance before this arrangement/agreement is terminated. If the DoD FA determines that the issues that led to the removal of the Federation member from the federation manager approval list have been resolved, the Federation member may be re-instated. In the event that the issues cannot timely be resolved, termination of this arrangement/agreement is the sole remedy of DoD FA for any alleged violation or non-compliance by the Federation member of the terms of this arrangement/agreement.

8.0 Voluntary Termination.

a. The Federation member may choose to terminate this arrangement/agreement and discontinue operation of its IDP for its convenience and in its sole discretion or may choose to no longer have its assertions approved for use by DoD Relying Parties, at any time, by giving written notice to the DoD FA not less than one hundred and twenty (120) calendar days prior to the date such termination is to be effective.

b. The DoD FA, for its convenience and in its sole discretion, may choose to terminate this arrangement/agreement and terminate approval for DoD Relying Parties accepting assertions issued by the Federation member at any time by giving written notice to the Federation member not less than one hundred and twenty (120) calendar days prior to the date such termination is to be effective.

9.0 Effect of Termination.

To the extent permitted by law, and notwithstanding anything herein to the contrary, any termination of this arrangement/agreement shall not provide a cause of action against any party to this Agreement. Each Party shall be solely responsible for its own costs and any damages it incurs as a result of termination of this arrangement/agreement.

10. Term.

This arrangement/agreement will remain in effect for a period of six (6) years from the last date of signature of this agreement. The parties shall perform an annual review of the terms of this arrangement/agreement to assure that all information is current, and documentation provided to the FPMWG

11. Modification and Renewal.

If at any time, any Party to this arrangement/agreement desires to modify it for any reason, that Party shall notify the other Party in writing of the proposed modification and the reasons for said modification(s). No modification shall occur unless there is written acceptance by both Parties hereto.

12. Liability.

Termination is the sole remedy for violation of the terms of this arrangement/agreement. This arrangement/agreement is entered into for the convenience of the Parties and, to the extent permitted by law, shall not give rise to any cause of action by the Parties hereto or by any third party, such as **user**s, for a violation of the terms of this arrangement/agreement. The federation member and its subordinates to this arrangement/agreement shall hold the Government harmless with respect to any liability arising out of the operation of the Federation member. In no event shall the DoD FA or the Department of Defense be liable for the payment of any subscription or service fees to the Federation member.

13. Disputes.

The Parties agree to resolve all claims, disputes, and other matters in question arising out of this arrangement/agreement, by good faith negotiations. Initial negotiations shall begin at the lowest level capable of problem resolution. If the parties cannot resolve the dispute at a lower level, the final arbiter of the dispute will be the DoD FA. The Federation member agrees to be bound by the DoD FA's final decision.

14. Governing Law.

The construction, validity, performance, and effect of this Agreement shall be governed by United States Federal law. This Agreement is entered into in the United States of America and shall not give rise to jurisdiction in any other country. {NOTE: Check with OGC on this paragraph}

15. Disclaimer.

This arrangement/agreement shall constitute the entire Agreement of the Parties. No prior or contemporaneous communications, oral or written, or prior drafts shall be relevant for purposes of determining the meaning of any provisions herein in any dispute or any other proceeding.

16. Severability.

If any terms or provisions of this arrangement/agreement prove to be invalid, void, or illegal, they shall in no way impair or invalidate any other terms or provisions herein, and the remaining terms and provisions shall remain in force.

17. Successors.

In the event either Party reorganizes or merges with another organization, or otherwise operates under new organizational control, this arrangement/agreement shall not apply to the succeeding organization(s) unless amended in writing by both parties. In the absence of an amendment, the trust relationship established herein shall terminate on the date of any status change.

18. Effective Date.

This arrangement/agreement is effective upon signature by both Parties hereto and shall remain in effect until termination or expiration.

19. Confidentiality.

Each Party shall keep in confidence and shall not disclose to any person or entity not bound by this arrangement/agreement, or make unauthorized use of, any appropriately marked business confidential or proprietary information provided by the other Party. Each Party shall use the same degree of care to protect the other Party's information as it uses to protect its own similar class of information. Termination of this arrangement/agreement shall not relieve the Parties from obligations to continue to protect against the disclosure of such confidential or proprietary information provided under this Agreement.

20. Nature of Agreement

This Agreement does not express or imply any commitment to purchase or sell goods or services or conduct of any business transaction.

1) Signatures

____

(Federation Authority of the Federation member)

____

(Date)

____

(Printed Name)

____

(Title)

____

(DoD Federation Authority)

____

(Date)

____

(Printed Name)

DoD CIO

____

(Title)