BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
MANUAL 36-3026

15 AUGUST 2024

Personnel

MISSION PARTNER IDENTITY, CREDENTIALING, AND ACCESS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A1P

Certified by: SAF/MR

Supersedes: DAFMAN36-3026, 11 January 2022

Pages: 18

This manual implements Department of the Air Force Policy Directive (DAFPD) 36-30, *Military Entitlements,* Department of the Air Force Instruction (DAFI) 36-3026, Volume 1 (V1), *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members and Other Eligible Personnel,* and DAFI 36-3026, Volume 2 (V2), *Common Access Card (CAC).* This manual specifically provides guidance based on Department of Defense Instruction (DoDI) 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*; Department of Defense Manual (DoDM) 1000.13, V1, *DoD Identification (ID) Cards: ID Card Life-Cycle*; DoDM 1000.13, V2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Members*; regarding background vetting and suitability to qualify for enrollment in the Defense Enrollment Eligibility Reporting System (DEERS) via the Mission Partner Identity, Credentialing, and Access Management (MP-ICAM), formerly Trusted Associate Sponsorship System (TASS) program. In collaboration with the Chief of Air Force Reserve (AF/RE), the Director of the Air National Guard (NGB/CF), and the Deputy Chief of Space Operations for Human Capital (SF/S1), the Deputy Chief of Staff for Manpower, Personnel, and Services (AF/A1) develops personnel policy for the Department of the Air Force DAF MP-ICAM. This publication applies to all civilian employees, uniformed members of the Regular Air Force (RegAF), the Air Force Reserve (AFR), the Air National Guard (ANG), United States Space Force (USSF), and those with a contractual obligation to abide by the terms of DAF publications (e.g., contractors). This manual requires the collection and or maintenance of information protected by the Privacy Act of 1972 authorized by DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*. The applicable System of Records

Notice (SORNs), Defense Manpower Data Center (DMDC), 02 DoD, Defense Enrollment Eligibility Reporting System (DEERS), are available at **http://dpclo.defense.gov/Privacy/SORNs.aspx**. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program,* and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command. This publication may not be supplemented. The authorities to waive wing, unit, or delta level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, and T-3") number following the compliance statement. See Department of the Air Force Manual 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Waiver requests will be submitted using the DAF Form 679, *Department of the Air Force Publication Compliance Item Waiver Request/Approval*, or via e-mail or memorandum if the form is unavailable. Additional information can be found within the D*AF MP-ICAM Standard Operating Procedures (SOP)*, which is continually refined and revised to ensure the MP-ICAM program changes are accurate and up to date. Compliance with **Attachment 2** in this publication is mandatory. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Department of the Air Force.

SUMMARY OF CHANGES

This publication has been revised to introduce Mission Partner-Identity, Credential, Access, and Management (MP-ICAM) as a replacement to Trusted Associated Sponsorship System (TASS).

Chapter 1

MP-ICAM INTRODUCTION

1.1. Purpose.

1.1.1. Overview. The Mission Partner Identity, Credentialing, and Access Management (MP-ICAM), will be used to register applicants, administer, and manage personnel under contract, volunteer, internship, or other support for base missions. **(T-0)** MP-ICAM primarily automates the verification and re-verification of employment sponsorship or affiliation, collection of personal information, and the MP-ICAM applicant enrollment in the Defense Enrollment Eligibility Reporting System (DEERS). In this instance, the DEERS program supports Common Access Card (CAC), Volunteer Logical Access Credential (VoLAC), NiPRNet (Non-classified Internet Protocol Router Network) Enterprise Alternative Token System (NEATS), and Uniformed Services Identification (USID) card issuances at Real-time Automated Personnel Identification System (RAPIDS) site locations.

1.1.2. Background. MP-ICAM administration and management must comply with guidance published in DoDM 1000.13, V1, which provides the minimum roles, responsibilities, and actions that must be accomplished in the workplace. **(T-1)** Refer to AFPC MP-ICAM SharePoint® for guidance information: **https://usaf.dps.mil/sites/afpc-home/DP3/DEERS**, or contact **DAF.MPICAM.WORKFLOW@us.af.mil**.

1.1.3. MP-ICAM Command and Installation Point of Contact (IPOC). Major Command (MAJCOM), Field Command (FLDCOM), Field Operating Agency or Direct Reporting Unit deputies must appoint in writing, a headquarters-level MP-ICAM administrator. **(T-1)** Installation commanders must appoint an IPOC in writing. **(T-1)** Refer to **Chapter 2**, Roles, and Responsibilities.

1.2. Variances, Exemptions, Exceptions to Policy (ETP). The affected work center shall process a request for variance, exemption, or ETP when it is impossible to meet DoD guidance due to operational needs, mission impact, or technical reasons. **(T-1)** Submit requests for variances, exemptions, or ETPs to DAF MPICAM Workflow at **DAF.MPICAM.workflow@us.af.mil**. A template (sample email) is provided in **Attachment 2**. When requesting a variance or exemption, or ETP, the work center leadership must provide the following:

1.2.1. Information identifying the operational needs, mission impact, or technical reasons; **(T-1)** and,

1.2.2. An implementation plan for interim control measures to reduce the degree of risk associated in order to protect personnel and property, equipment and systems, and physical and logical accesses. **(T-1)**

1.3. Applying Standards. This DAFMAN establishes the minimum standards for incorporating parts of the DoDI 1000.13; DoDM 1000.13, V1 & V2; and DAFI 36-3026, V1 and V2 related to DAF MP-ICAM operations.

1.4. How to Use This Manual. MP-ICAM administrators, managers, and sponsors are required to comply with applicable DoD instructions, manuals, and guides for the MP-ICAM program, and DAF MP-ICAM SOP along with this manual. A list of applicable publications are listed in **Attachment 1**. For compliance, this manual is supported by the Management Internal Control

Toolset (MICT) as a DAF standard. The MICT contains checklist items important to overall MP-ICAM administration success. Refer the AF MP_ICAM SharePoint®: **https://usaf.dps.mil/sites/afpc-home/DP3/DEERS** checklist items. For any legal issues or questions regarding this manual, contact your servicing legal office.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. General Information. This chapter provides general MP-ICAM work center procedures and personnel roles assigned within MP-ICAM. Each role requires individuals be a US citizen and a government employee, military, or DoD civilian. All individuals must also possess a valid security clearance and CAC.

2.2. MAJCOM/FLDCOM/CC or designee: Appoints MP-ICAM Administrators in writing. Assigns responsibility for administration and management of the MP-ICAM program to installation commanders (or designees) at each installation operating an MP-ICAM program.

2.3. Installation Commander. Installation commanders are responsible for identifying an Installation Point of Contact (IPOC) for establishing the MP-ICAM administration and management. The MP-ICAM administration and management is role-based assigned by the Defense Manpower Data Center (DMDC). MP-ICAM roles include the Mission Partner Affiliation Security Manager (MPASM) and Mission Partner Affiliation Sponsor (MPAS). This role-base establishes a MP-ICAM hierarchal standard for responsiveness, and provides uniform guidance, which the IPOC, MPASM and MPAS may supplement to meet more stringent local mission requirements.

2.4. Installation Point of Contact (IPOC). The IPOC is identified in writing by the Installation Commander or designee for establishing the MP-ICAM administration and management.

2.4.1. The IPOC will ensure MPASM meets requirements for appointment as stated above. Refer to DAF MP-ICAM SOP for submitting a Department of Defense (DD) Form 2875, *System Authorization Access Request* to the DAF MP-ICAM Service Point of Contact (SPOC).

2.4.2. The MPASM will be appointed by the IPOC in writing, and the DD Form 2875 sent to DAF MP-ICAM SPOC.

2.4.3. The IPOC will add or remove MPASM s as a result of Permanent Change of Station (PCS), Temporary Duty (TDY) when impacting MP-ICAM duties, separation, retirement, etc.

2.5. Mission Partner Affiliation Security Manager (MPASM).

2.5.1. The MPASM will upload appointed Mission Partner Affiliation Sponsor (MPAS) into the MP-ICAM via DMDC Enterprise Monitoring Management of Accounts application (refer to DAF MP-ICAM SOP for submitting a DD Form 2875).

2.5.2. The MPASM will conduct site visit verification of the appointed MPAS when necessary to ensure local mission requirements are met to satisfy MP-ICAM administration support to eligible contractor, volunteer, intern, and other eligible populations.

2.5.3. The MPASM will add or remove MPASs as required due to PCS, separation, etc.

2.5.4. The MPASM will administer semi-annual or refresher training at any time to address MPAS deficiency.

2.6. Mission Partner Affiliation Sponsor (MPAS). The MPAS will be appointed by letter from the unit of responsibility (refer to DAF MP-ICAM SOP for submitting a DD Form 2875 to respective MPASM). The MPAS will:

2.6.1. Add or remove contractors, volunteers, interns, and other eligible populations in MP-ICAM.

2.6.2. Ensure contractors and other eligible populations meet security requirements according to the guidelines contained in DAF MP-ICAM SOP.

2.6.3. Ensure contractors and other eligible populations have a requirement to access DoD computers to accomplish duties before creating a MP-ICAM application enrollment for DEERS, authorizing issuance of the CAC.

2.6.4. Enroll contractors and other eligible populations into MP-ICAM after verifying contract number and start and expiration date.

2.6.5. Re-verify contractor status every 6 months or 180 days in MP-ICAM.

2.6.6. Delete and remove personnel at the end of contract or at the end of the contractors' employment or termination, and recover CACs issued to contractors and other eligible populations according to AFPC MP-ICAM Form 2 (refer to DAF MP-ICAM SOP).

2.6.7. Report to respective Contracting Officer Representative (COR) or OPR when contractors and other eligible populations do not turn in their CACs.

2.6.8. Return terminated CACs to the Force Support Squadron (FSS), Customer Service office or nearest RAPIDS facility for return to the Defense Manpower Data Center (DMDC).

2.7. MP-ICAM User Role – General Information. The MP-ICAM user roles are hierarchal functions and based on a DoD enterprise approach for managing contractor and other eligible populations within the MP-ICAM program. In this instance, the user role correlates to the military or civilian MP-ICAM MPAS and the government sponsor who is requesting the contractor or other eligible populations for enrollment within the MP-ICAM program.

2.7.1. The CAC, VoLAC, USID, and NEATS card issuances are based on the MP-ICAM MPAS actions to create an application on behalf of an eligible person, and approve the person for DEERS enrollment, and for the person to receive the appropriate type of card from a RAPIDS site (ID card issuance facility).

2.7.2. Further details of the MP-ICAM user roles are listed at paragraphs **3.5** through **3.5.5**., MP-ICAM Service User Role Description.

2.8. Contracting Officer Representative (COR). The Government sponsor organization that the contract supports nominates the COR and the Contracting Officer appoints the COR by letter. The COR is the representative acting on behalf of the Government sponsor organization. Examples of COR responsibilities are found in DoDI 5000.72, *DoD Standard for COR Certification*, Encl 6, Table 1; in DAFI 63-138, *Acquisition of Services*, Para 2.13; and in the DoD COR Guidebook, and include:

2.8.1. Ensure the necessary requirements are met for contractor background checks and all other required security clearances (if applicable).

2.8.2. Monitor contractor compliance with security.

2.8.3. Review contractor requests for government assets.

2.8.4. Coordinate and provide any government-owned (or leased) assets (CACs are government assets) or use of U.S. Government space to the contractor as required by the contract.

2.8.5. Monitor the control and disposition of any government-furnished assets. Ensure the completion of all required documentation for the acceptance, use, and return of government-furnished assets, including unique identification tracking.

2.8.6. Provide to the contracting officer an assessment of any loss, damage, or destruction of U.S. Government property.

2.8.7. Verify and provide to the Mission Partner Affiliation Sponsor (MPAS) all contract and contractor personnel information the MPAS needs.

2.8.8. Monitors and maintains copies of contractor support records for Government furnished equipment (GFE), security clearances, CACs, travel requests, travel reports, and all billing/payment documents. Makes these records available for Contracting Officer (CO) review any time requested.

Chapter 3

MP-ICAM AUTHORITIES AND RESPONSIBILITIES

3.1. MP-ICAM Authorities. This chapter provides additional information of MP-ICAM authorities supporting the establishment and administration of the MP-ICAM program.

3.1.1. The Department of the Air Force authority to administer the MP-ICAM program is derived from the DoDM 1000.13, V1.

3.1.2. MP-ICAM is the DoD uniformed services and agency DEERS registration platform for enrolling qualifying contractors, volunteers, interns, and others according to DoDM 1000.13, V1. MP-ICAM shall serve as the sponsorship and DEERS data registration tool for CAC-eligible DoD contractors and other populations as determined by the Director, Defense Human Resources Activity (DHRA). **(T-0)** MP-ICAM employs an automated version of the DD Form 1172-2, *Application for Identification Card/DEERS Enrollment*, to collect information necessary for DEERS enrollment. Organizations that use MP-ICAM must adhere to the guidelines on user roles in accordance with DoDM 1000.13, V1. **(T-0)**

3.1.3. The DAF Service Point of Contact (SPOC) shall be a member of AFPC/DP3SA. **(T-0)** The SPOC shall coordinate with the DMDC to establish a site with MP-ICAM capability. **(T-0)** The SPOC will create policies, operating procedures and supporting documentation for DAF implementation. **(T-0)** The SPOC will oversee MPASM registration and provide any other required field support. **(T-0)**

3.1.4. The DAF MP-ICAM SPOC duties and responsibilities are supported by the DAF project officer. **(T-0)** The DAF project officer is appointed in accordance with DoDI 1341.02, *DEERS Program and Procedures*.

3.2. DAF MP-ICAM Guidance. DAF MP-ICAM guidance is contained within this manual and in the DAF MP-ICAM Standard Operation Policy and Procedures (SOP) guidance. The DAF MP-ICAM SOP is a document published by the DAF MP-ICAM SPOC. The DAF MP-ICAM SOP directly supports MP-ICAM site operations, including MPASM and MPAS administration processes and procedures according to DoDM 1000.13, V1. The SOP is subject to change without notice and must be checked often at the DAF MP-ICAM SharePoint®: **https://usaf.dps.mil/sites/afpc-home/DP3/DEERS/SitePages/Home.aspx**.

3.3. MP-ICAM System of Record. The MP-ICAM program is recognized as a system of record within the DMDC program enterprise to sponsor contractors, volunteers, interns, and other eligible populations for DEERS enrollment, including CAC and USID card issuances. This authority is derived from the DoDM 1000.13, V1.

3.3.1. Service Point of Contact (SPOC). The MP-ICAM SPOC:

3.3.1.1. Must be a U.S. citizen. **(T-0)**

3.3.1.2. Must be a uniformed services member, civilian employee working for the sponsoring organization, or a DoD contractor providing management support to the service or agency implementing MP-ICAM (a contractor cannot perform the MPAS or MPASM role). **(T-0)**

3.3.1.3. Must be capable of sending and receiving digitally signed and encrypted e-mail. **(T-0)**

3.3.1.4. Must be a CAC holder. **(T-0)**

3.3.1.5. Shall complete the training provided by DMDC for the MPASM and MPAS roles. **(T-0)**

3.3.2. The MPASM will act as a MPAS and oversee the activity for MP-ICAM site MPASs. **(T-0)** A MP-ICAM MPASM:

3.3.2.1. Must be a U.S. citizen. **(T-0)**

3.3.2.2. Must be a uniformed services member or a DoD civilian employee working for the sponsoring organization. **(T-0)**

3.3.2.3. Must be capable of sending and receiving digitally signed and encrypted e-mail. **(T-0)**

3.3.2.4. Must be a CAC holder. **(T-0)**

3.3.2.5. Shall complete the training provided by DMDC for the MPASM role. **(T-0)**

3.3.2.6. At a minimum, MPASMs shall conduct annual audits and oversight functions of their specific MPAS. **(T-0)**

3.3.3. MPAS. MPAS's shall be sponsors for eligible populations within MP-ICAM and will utilize MP-ICAM to register data for the DD Form 1172-2, re-verify CAC, VoLAC, NEATS, or USID card holder affiliation, and revoke credentials, e.g., CACs in accordance with this manual and the DMDC MP-ICAM User Guide. **(T-0)** Sponsoring an applicant is a multi-step process which includes establishing the individual's eligibility and verifying the individual has the necessary background investigation completed to be issued a CAC. **(T-0)** A MP-ICAM MPAS:

3.3.3.1. Must be a U.S. citizen. **(T-0)**

3.3.3.2. Must be a uniformed services member, a DoD civilian employee working for the sponsoring organization, or a non DoD Federal agency employee approved by DHRA. **(T-0)**

3.3.3.3. Must be capable of sending and receiving digitally signed and encrypted e-mail. **(T-0)**

3.3.3.4. Must be a CAC holder. **(T-0)**

3.3.3.5. Shall complete the training provided by DMDC for the TA role. **(T-0)**

3.3.3.6. Shall manage no more than 100 active applicants (contractors and others) at any given time within MP-ICAM. **(T-0)** Exceptions to this limit can be authorized by the DoD Component concerned to address specific contract requirements that substantiate a need for a larger contractor-to- MPAS ratio. The DoD Component SPOC shall document any authorized exceptions to the 100-contractors limit. **(T-0)** MPASMs and MPASs refer to the DAF MP-ICAM SOP for requesting waivers to their IPOC.

3.3.3.7. Shall coordinate with their contracting personnel when establishing the contractor's initial and continued affiliation with DoD and need for CACs in accordance with agency or Component-level procedures. **(T-0)**

3.3.3.8. Shall coordinate with their contracting, human resources, or personnel security organizations to confirm that the appropriate background check has been completed for CAC applicants. **(T-0)**

3.3.3.9. Shall re-verify a CAC, VoLAC, NEATS, or USID card holder's need for a credential every 6 months (180 days) within MP-ICAM. **(T-0)**

3.3.3.10. Shall revoke the CAC, VoLAC, NEATS, or USID card within the MP-ICAM upon termination of employment or completion of affiliation with the DoD. **(T-0)**

3.3.3.11. Shall ensure that the CAC, VoLAC, NEATS, or USID card is retrieved upon the CAC holder's termination of employment or completion of affiliation with the DoD. **(T-0)**

3.4. MP-ICAM Service User Compliance. MP-ICAM user roles authority is derived from DoDI 1341.02. MP-ICAM is the sponsorship and DEERS registration tool for eligible DoD contractors and other affiliated populations as determined by the Director, DHRA (Defense Human Resources Activity). MP-ICAM collects eligibility and enrollment information and serves as the authoritative source for DoD contractors and other affiliated populations as determined by the Director, DHRA. Organizations that use MP-ICAM must adhere to requirements and guidelines on user roles outlined in DoDI 1341.02. **(T-0)**

3.5. MP-ICAM Service User Role Description. The DAF MP-ICAM Service user roles and responsibilities are derived from DoDM 1000.13, V1; stating the user:

3.5.1. Shall coordinate with their contracting personnel when establishing the contractor's initial and continued affiliation with DoD and need for CACs in accordance with agency or component level procedures. **(T-0) Example:** The MPAS will obtain a completed Air Force Personnel Center Airmen Support Branch (AFPC/DP3SA) MP-ICAM, *Contractor CAC Issuance – Form 1* from the government sponsor and verify that the government sponsor has completely filled out Section II certifying that the applicant requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the sponsoring government organization for a period of 6-months or more (applicable to DoD contractors only) and if the applicant requires access to both DoD facilities and logon access to DoD Networks on site or remotely. **(T-0)** (A typical government sponsor is a Contracting Officer Representative (COR) with authority to provide oversight of the contract personnel as they conduct business in accordance with the performance work statement).

3.5.2. Shall coordinate with their contracting, human resources, or personnel security organizations to confirm the appropriate background check has been completed for CAC applicants in accordance with the AFPC/DP3SA MP-ICAM Form 1. **(T-0) Example:** The MPAS will verify the AFPC/DP3SA MP-ICAM Form 1 from the government sponsor is signed in Section III by a Security Manager verifying the applicant meets the vetting criteria. **(T-0)**

3.5.3. Shall re-verify a CAC holder's need for a CAC every 6 months (180 days) within MP-ICAM. **(T-0) Example:** The MPAS will request an AFPC/DP3SA MP-ICAM *CAC Reverification / Retrieval Form 2* from the government sponsor ensuring that section I and II

are filled out properly. **(T-0)** If the form is filled out properly, MPAS will login to MP-ICAM and re-verify the applicant. **(T-0)**

3.5.4. Shall revoke the CAC within MP-ICAM upon termination of employment or completion of affiliation with the DoD. **(T-0) Example:** The MPAS will be notified by the government sponsor that a contractor has been terminated or is no longer affiliated with the DoD by providing the MPAS an AFPC/DP3SA MP-ICAM Form 2, with Section I and II filled out. **(T-0)**

3.5.5. Shall ensure that the CAC is retrieved upon the CAC holder's termination of employment or completion of affiliation with the DoD. **(T-0**) **Example:** The MPAS will be notified by the government sponsor that a contractor or volunteer has been terminated or is no longer affiliated with the DoD by providing the MPAS an AFPC/DP3SA MP-ICAM Form 2, with Section I filled out. **(T-0)** Section III of AFPC/DP3SA MP-ICAM Form 2 contains blocks to enter the date the CAC was revoked, retrieved, and given to the RAPIDS/DEERS (ID Card Facility) site in the lower portion of the section. A MPAS or MPASM must enter their name, date, and electronically sign this portion of the form to complete the CAC retrieval process after the MPAS /MPASM has verified with the local COR that the CAC was retrieved and given to the nearest DEERS/RAPIDS site. **(T-0)** Examples of other eligible MP-ICAM populations administratively supported:

3.5.5.1. AFPC/DP3SA MP-ICAM *Foreign Affiliate CAC Issuance-Form 3*.

3.5.5.2. AFPC/DP3SA MP-ICAM *Foreign Affiliate CAC Reverify/Retrieval-Form 4*.

3.5.5.3. AFPC/DP3SA MP-ICAM *Foreign Affiliate USID/NEATS Issuance-Form 5*.

3.5.5.4. AFPC/DP3SA MP-ICAM *Foreign Affiliate USID/NEATS Reverify/Retrieval-Form 6*.

3.5.5.5. AFPC/DP3SA MP-ICAM *Volunteer, Intern, SMART, Key Spouse, Other NEATS Issuance-Form 7*.

3.5.5.6. AFPC/DP3SA MP-ICAM *Volunteer, Intern, Key Spouse, SMART and Other Individual Reverify/Retrieval-Form 8*.

ALEX WAGNER
Assistant Secretary of the Air Force
(Manpower and Reserve Affairs)

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 USC § 3111, *Acceptance of volunteer service*

10 USC §1588, *Authority to accept certain voluntary services*

DoDD 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, 20 April 1999

DoDI 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, 23 January 2014

DoDI 1341.02, *Defense Enrollment Eligibility Reporting System (DEERS) Program and Procedures*, 18 August 2016

DoDI 1100.21, *Voluntary Services in the Department of Defense*, 27 March 2019

DoDI 5000.72, *DoD Standard for Contracting Officer Representative Certification*, 26 March 2015

DoDI 5200.46, *DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)*, 9 September 2014

DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, 8 December 2020

DoDM 1000.13, V1, *DoD Identification (ID) Cards*: *ID Card Life-Cycle*, 23 January 2014

DoDM 1000.13, V2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Members*, 23 January 2014

DoDM 5200.02, *Procedures for the DoD Personnel Security Program (PSP)*, 3 April 2017

DAFPD 36-30, *Military Entitlements*, 25 April 2023

DAFI 36-3026, V1, *Identification Cards For Members Of The Uniformed Services, Their Eligible Family Members And Other Eligible Personnel*, 1 June 2023

DAFI 36-3026, V2, *Common Access Card*, 24 January 2023

DAFI 63-138, *Acquisition of Services*, 2 January 2024

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 October 2023

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

DAF Mission Partner-Identity, Credential and Access Management (MP-ICAM) Standard Operating Procedures (SOP)

Department of Defense (DoD) Contracting Officer Representatives (COR) Guidebook, October 2022

DMDC MP-ICAM User Guide

USD P&R Memorandum, *Logical Access Credentials for DoD Volunteers*

Prescribed Forms

None

Adopted Forms

AFPC/DP3SA MP-ICAM *Contractor CAC Issuance-Form 1*

AFPC/DP3SA MP-ICAM *Contractor CAC Reverify/Retrieval-Form 2*

AFPC/DP3SA MP-ICAM *Foreign Affiliate CAC Issuance-Form 3*

AFPC/DP3SA MP-ICAM *Foreign Affiliate CAC Reverify/Retrieval-Form 4*

AFPC/DP3SA MP-ICAM *Foreign Affiliate USID/NEATS Issuance-Form 5*

AFPC/DP3SA MP-ICAM *Foreign Affiliate USID/NEATS Reverify/Retrieval-Form 6*

AFPC/DP3SA MP-ICAM *Volunteer, Intern, SMART, Key Spouse, Other NEATS Issuance-Form 7*

AFPC/DP3SA MP-ICAM Volunteer, Intern, Key Spouse, SMART and Other Individual Reverify/Retrieval-Form 8

DAF Form 679, Department of the Air Force Publication Compliance Item Waiver Request/Approval

DAF Form 847, Recommendation for Change of Publication

DD Form 1172-2, Application for Identification Card/DEERS Enrollment

DD Form 2875, *System Authorization Access Request*

SF 85, *Questionnaire for Non-sensitive Positions*

SF 85-P, *Questionnaire for Public Trust Positions*

SF-86, *Questionnaire for National Security Positions*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFR—Air Force Reserve

ANG—Air National Guard

CAC—Common Access Card (smart-card)

CO—Contracting Officer

COR—Contracting Officer Representative

CVS—Contractor Verification System

DAF—Department of the Air Force

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

DEERS—Defense Enrollment Eligibility Reporting System

DD—Department of Defense

DHRA—Defense Human Resources Activity

DMDC—Defense Manpower Data Center

DoD—Department of Defense

DODI—Department of Defense Instruction

DODM—Department of Defense Manual

ETP—Exception to Policy

FLDCOM—Field Command

GFE—Government Furnished Equipment

ID—Identification

IP—Internet Protocol

IPOC—Installation Point of Contact (for MP-ICAM)

MAJCOM—Major Command

MICT—Management Internal Control Toolset

MP-ICAM—Mission Partner Identity, Credentialing, and Access Management

MPAS—Mission Partner Affiliation Sponsor

MPASM—Mission Partner Affiliation Security Manager

NGB—National Guard Bureau

NEATS—NIPRNet Enterprise Alternative Token System

NiPRNet—Non-classified Internet Protocol Router Network

OPR—Office of Primary Responsibility

PCS—Permanent Change of Station

PIRR—Participating Individual Ready Reserve

PIV—Personal Identity Verification

PKI—Public Key Infrastructure

RAPIDS—Real-time Automated Personnel Identification System

SF—Standard Form

SJA—Staff Judge Advocate

SOP—Standard Operating Procedures

SORN—System of Records Notice

SPOC—Service Point of Contact

SSN—Social Security Number

TASS—Trusted Associate Sponsorship System transitioned to MP-ICAM

TCP—Transmission Control Protocol

TDY—Temporary Duty

USID—Uniformed Services Identification Card (non smart-card)

USSF—U.S. Space Force

VoLAC—Volunteer Logical Access Credential (smart-card)

V1—Volume 1

V2—Volume 2

Office Symbols

AF/A1—Deputy Chief of Staff for Manpower, Personnel, and Services

AF/A1P—Chief, Force Management Policy Directorate

AF/A1PP—Chief, Military Force Policy Division

AF/RE—Chief of Air Force Reserve

AFPC/DP3SA—Air Force Personnel Center Special Programs Branch

SAF/MR—Assistant Secretary of the Air Force for Manpower, Personnel, and Services

SF/S1—Deputy Chief of Space Operations for Human Capital

Terms

Common Access Card—Smart card-based technology and systems used to transform and improve security in DoD processes and mission performance, thereby, enhancing readiness while also improving business processes. The standard ID card for AD uniformed services personnel (to include the Selected Reserve), Participating Individual Ready Reserve (PIRR), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals. The Department's primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment. It is the principal card enabling physical access to buildings, facilities, installations, and controlled spaces. See DAFI 36-3026, V2.

Contractor—A non-government employee under contract or working for a firm under contract with the DoD, or Uniformed Services.

Defense Enrollment Eligibility Reporting System (DEERS)—A computer-based enrollment and eligibility system that the DoD established to support, implement, and maintain its efforts to improve planning and distributing military benefits, including military health care, and to eliminate waste and fraud in the use of benefits and privileges. DEERS can interact with and support systems and programs within DoD and the military departments.

DoD Beneficiary—A person who receives benefits from the DoD based on a prior association, condition, or authorization (see unremarried widow and unremarried former spouse). DoD Beneficiary prior association, condition, or authorization does not allow for extending DEERS

eligibility to other populations for the purposes of qualifying for benefits or privileges associated with the ID card.

DoD Identification Number—Replaces the SSN with a 10-digit DoD number to every person with a direct relationship with the DoD.

In AD Training—A period of training on active duty which includes not only that time between muster and dismissal, but also includes travel to or from such drills.

Installation Point of Contact (IPOC)—Installation commanders are responsible for identifying an IPOC for establishing the MP-ICAM administration and management.

Installation Security Authority—Army - Military Police; Navy - Military Police; Air Force - Security Forces (includes U.S. Space Force); Marine Corps - Provost Marshal.

Internet—The Internet is a global system of interconnected computer networks using Standard Internet Protocol (IP) suite, Transmission Control Protocol (TCP/IP) to connect and exchange information.

Public Key Infrastructure (PKI)—A support service to the Personal Identity Verification (PIV) system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

Installation Commander—For the purpose of this DAFMAN, the following defines the senior installation official for the seven Uniformed Services:

Army - Installation Commander
Navy - Commanding Officer
Air Force - Support Group Commander (includes U.S. Space Force)
Marine Corps - Commanding General, Commanding Officer (as appropriate)
Coast Guard - Commanding Officer
National Oceanic and Atmospheric Administration - Commanding Officer
United States Public Health Service - Officer in Charge

Service Member—An individual who is affiliated with the United States Uniformed Services, either AD, Reserve, or Guard or a retiree entitled to retired or retainer pay.

Sponsor—Eligible beneficiary (see DAFI 36-3026, V1, Attachment 2) with dependents. The prime beneficiary who derives his or her eligibility based on individual status rather than dependence upon another person. This beneficiary receives benefits based on his or her direct affiliation to the DoD.

Staff Judge Advocate (SJA)—Staff Judge Advocate or other judge advocate or civilian attorney in the servicing Office of the Staff Judge Advocate.

System of Records Notice (SORN)—A formal notice to the public published in the Federal Register that identifies the purpose for which Personally Identifiable Information (PII) is collected, from whom, what type, how information is shared, and how to access and correct information maintained by the agency.

Tier Waiver Approval Authorities—Waiver approval authorities are indicated by Tier numbers (T-0, T-1, T-2, and T-3) following compliance statements. Refer to DAFMAN 90-161, Chapter 9 and Table A10.1 for additional guidance on waiver authorities and the waiver process. (Not to be confused with security investigation tier levels defined below).

Tier Security Investigations—The DoD CAF, in alignment with DoDM 5200.02 - *Procedures for the DoD Personnel Security Program (PSP)* and DoDD 5220.6 - *Defense Industrial Personnel Security Clearance Review Program*, is standardizing the process for adjudicating Personnel Security Investigations for eligibility and access to classified information. Reference Defense Counterintelligence and Security Agency. See Tier levels below.

Tier 1—(uses the Standard Form (SF) 85, *Questionnaire for Non-sensitive Positions*) and is the investigation for positions designated as low-risk, non-sensitive. It is also the minimum level of investigation for a final credentialing determination for physical and logical access. Tier 1 investigations are requested using the SF 85.

Tier 2—(uses the SF-85P, *Questionnaire for Public Trust Positions*) and is the investigation for non-sensitive positions designated as moderate risk public trust positions. Tier 2 investigations are requested using the SF 85P. (**Note**: Tier 2 security investigation applies to MP-ICAM MPASM, MPAS, and CAC/VoLAC eligible populations.)

Tier 3—(uses the SF-86, *Questionnaire for National Security Positions*) and the investigation (T3) formerly National Agency Check with Local Agency Check and Credit designed as the initial investigation for contractors at the Confidential and Secret national security access levels.

Tier 4—(uses the SF-85P form) for non-sensitive High Risk (Public Trust) positions.

Tier 5—(uses the SF-86 form), formerly Single Scope Background Investigation, this is the government-wide investigation required of those who need access to Top Secret classified national security information.

Uniformed Services—The Army, Navy, Air Force, Space Force, Marine Corps, Coast Guard, National Oceanic and Atmospheric Administration, and United States Public Health Service.

Uniformed Services Identification (USID) Card—Non smart card, identification leading to installation access and or benefits, and privileges.

Volunteer Logical Access Credential (VoLAC)—Reference USD P&R Memorandum, Logical Access Credentials for DoD Volunteers (Pilot Program); establishes the DEERS/RAPIDS programs as the source for issuing a logical access credentials to qualifying volunteers. Volunteer enrollment occurs within the Contractor Verification System (CVS) or MP-ICAM to the DEERS database. RAPIDS is the platform for issuing the credential for volunteers authorized by either 10 U.S.C. § 1588 or 5. U.S.C. § 3111. This credential has DoD PKI certificates used for authentication to DoD networks. See DoDI 1100.21, Voluntary Services in the Department of Defense.

Attachment 2

VARIANCES, EXCEMPTION, EXCEPTION TO POLICY (ETP) – SAMPLE EMAIL

A2.1. Sample Email - Variances, Exemption, Exception to Policy (ETP). The effected work center shall process a request for variance, exemption, or ETP when it is impossible to meet DoD guidance due to operational needs, mission impact or technical reasons. **(T-1)** When requesting a variance or exemption, or ETP, the work center leadership must provide the following:

A2.1.1. Identify the operational needs, mission impact, or technical reasons. **(T-1)**

A2.1.2. Implementation plan for interim control measures to reduce the degree of risk associated in order to protect personnel and property, equipment and systems, and physical and logical accesses. **(T-1)** Refer to **Figure A2.1**. Email to DAF MP-ICAM SPOC below:

Figure A2.1. Email to DAF MP-ICAM SPOC.

To: DAF MP-ICAM SPOC, AF DEERS RAPIDS MP-ICAM Tier 3
AFPC.DP3.AFDEERSRAPIDSTASS@us.af.mil

Subject: MP-ICAM Site ID (123456-Base Location) – Variances, Exemption, Exception to Policy (ETP)

We are unable to meet the DoD Guidance (DoDM 1000.13, Volume 1 or DoDI 5200.46) due to operational needs, mission impact, or technical reasons (explain in detail).

The following Operational Need(s) is provided:
The following Mission Impact(s) is provided:
The following Technical Reason(s) is provided:

The following implementation plan for interim control measures to reduce the degree of risk associated in order to protect personnel/property, equipment/system, and physical/logical accesses is provided.

Signed by: MP-ICAM Installation Point of Contact (IPOC) or designated MP-ICAM representative.