



MP ICAM Overview 15 MAY 2024

Mission Partner Identity Credential and Access Management (MP ICAM) Overview

Task

Provide an overview of MP ICAM

Purpose

Inform CORs and VREPs of MP ICAM Roles, Processes and Functionality

End State

Shared understanding of MP ICAM



Agenda

- What is MP ICAM?
- Relevance to the DOC PER Process
- MP ICAM Roles
- Steps to become an MPAS
- MPAS - Change of Custody
- Reverification
- Questions



What is MP ICAM?

- MP ICAM (Mission Partner Identity, Credential and Access Management) is a Defense Manpower Data Center (DMDC) sponsored and supported secure web-based application:
 - Released in September 2023 to replace TASS
 - Allows for the initiation, sponsorship and management of DoD and non-DoD Mission Partners for physical and logistical access or use of DoD systems and facilities, depending on the credential type and sponsorship
 - Verifies eligibility for issuance of Common Access Cards (CAC) to DoD Contractors
 - Authoritative data-feed for the Defense Enrollment Eligibility Reporting System (DEERS)



Relevance to the DOCPER Process

- Role of DD 1172-2s: DD Form 1172-2 is required (*in Germany and Italy*) for CAC issuance
- IMPORTANT: MP ICAM expiration date **MUST** = the date on the DD 1172-2 issued by DOCPER (block 33 on the 1172-2)
- The expiration date is based on whichever date comes first:
 - Contract Expiration Date
 - Passport Expiration Date
 - 3 years from the date 1172-2 was issued



MP ICAM Roles: DMDC

- Defense Manpower Data Center (DMDC) operates and maintains the MP ICAM infrastructure
- The DMDC helpdesk will assist with errors that often occur when provisioning the MPAS and issues with applications
- The 24-hour helpdesk number is 800-538-9522 or Commercial: 502-335-9980



MP ICAM Roles: SPOC

- The Service Point of Contact (SPOC) is the highest-level Sponsor
- SPOC responsibilities include:
 - Creation of the site
 - Facilitate transfer from one site to another (i.e. Army to Army)
 - Management of Sponsors at their site to include provisioning/updating/removing Sponsors accounts
 - Troubleshooting issues with accounts
 - Creating policies, operating procedures and supporting documentation in support of service or agency specific implementation
 - Coordinate any requests for new or additional MP ICAM responsibilities with DMDC



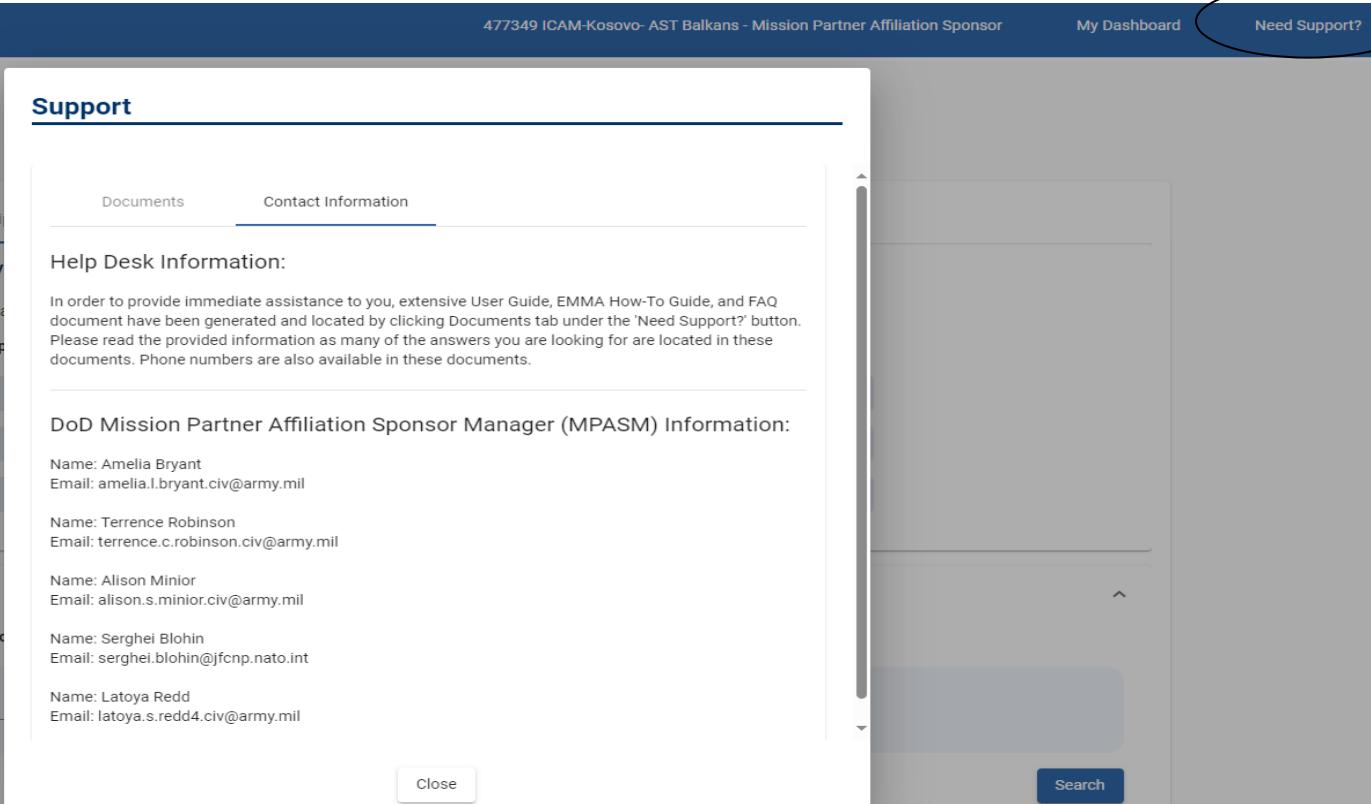
MP ICAM Roles: MPASM

- The Mission Partner Affiliation Sponsor Manager (MPASM) is appointed by the SPOC
- The MPASM is responsible for all activities associated with their site to include:
 - Provisioning the MPAS in EMMA as requested and manage lists of all active MPAS within the site
 - Ensuring applicants are managed appropriately throughout the credential sponsorship life cycle
 - Provide communication to their site (ie. Information about MP ICAM, meetings with SPOCs, send out newsletters from SPOC)
 - Provide assistance and training with any issues that arise among MPAS



MP ICAM Roles: MPASM

- MPAS can go to “Need Support” to find the site’s MPASMs Contact Info



The screenshot shows a web interface for '477349 ICAM-Kosovo- AST Balkans - Mission Partner Affiliation Sponsor'. At the top, there are tabs for 'My Dashboard' and 'Need Support?'. A yellow star highlights the 'Need Support?' button. A modal window titled 'Support' is open, showing tabs for 'Documents' and 'Contact Information'. The 'Contact Information' tab is selected, displaying 'Help Desk Information' and 'DoD Mission Partner Affiliation Sponsor Manager (MPASM) Information'. The MPASM information lists five contacts with their names and email addresses. At the bottom of the modal are 'Close' and 'Search' buttons.

Name	Email
Amelia Bryant	amelia.l.bryant.civ@army.mil
Terrence Robinson	terrence.c.robinson.civ@army.mil
Alison Minior	alison.s.minior.civ@army.mil
Serghei Blohin	serghei.blohin@jfcnp.nato.int
Latoya Redd	latoya.s.redd4.civ@army.mil

- If you still need support, please contact us:
usarmy.wiesbaden.usareur-af.mbx.odcs-g1-MP ICAM@army.mil



MP ICAM Roles: MPAS

- Mission Partner Affiliation Sponsor (MPAS) is provisioned by an MPASM
 - The MPAS seeking appointment needs to complete a DD 2875 (System Authorization Access Request) form and complete the required training to be provisioned
- Responsible for managing the complete lifecycle of credential sponsorship, to include:
 - Establishing sponsorship
 - Re-verifying the applicant (every 6 months)
 - Ensure all policy, procedures and requirements are met
- Helpful reminder. MPAS must log into MP ICAM every 30 days to stay active



Steps to Become an MPAS

- Requirements to become an MPAS:
 - Must be a US Citizen/ not been convicted of a felony or denied a security clearance
 - DoD Uniformed Service Member or DoD Civilian
 - FBI fingerprint check with favorable results
 - At minimum, a NACI background investigation completed
 - Be a CAC holder
 - Capable of sending and receiving digitally signed/encrypted email
 - Completed MP ICAM certification training (once provisioned!)



Steps to Become an MPAS (cont.)

- Email the MPASM team at the MP ICAM inbox:
usarmy.wiesbaden.usareur-af.mbx.odcs-g1-MP ICAM@army.mil
- Include a **completed** DD 2875 with digital signatures from the Supervisor and the Security manager with investigation information
- Once DD 2875 is reviewed by a MPASM, you will be provisioned in EMMA and a welcome email sent with instructions
- Complete the JKO training (DMDC-US1430-MPICAM)
- Wait **24 hours** from training completion to try logging in

UNCLASSIFIED		OMB No. 0704-0600 OMB approval expire: 2025-05-31
SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)		
PRIVACY ACT STATEMENT		
The public reporting burden for this collection of information, which is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. (less comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Information Headquarters Service, in which no new and/or cost information collecting will result. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.)		
AUTHORITY: Executive Order 14040; and Public Law 96-474, the Computer Fraud and Abuse Act		
PRINCIPAL PURPOSE(S): To record names, signature, and other identifiers for the purpose of validating theworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form		
ROUTINE USE(S): None		
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.		
TYPE OF REQUEST		DATE (YYYYMMDD) 20231107
<input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID		
SYSTEM NAME (Platform or Application) MP ICAM		LOCATION (Physical Location of System)
PART I (To be completed by Requester)		
1. NAME (Last, First, Middle Initial)		2. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT AEPE		4. PHONE (DSN or Commercial)
5. OFFICIAL E-MAIL ADDRESS		6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS		8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR		
10.1A TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)		
<input type="checkbox"/> I have completed the Annual Cyber Awareness Training.		DATE (YYYYMMDD)
11. USER SIGNATURE		12. DATE (YYYYMMDD)
PART II ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)		
13. JUSTIFICATION FOR ACCESS		
14. TYPE OF ACCESS REQUESTED <input type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED		
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER		
16. VERIFICATION OF NEED TO KNOW <input type="checkbox"/> I certify that this user requires access as requested.		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)
17. SUPERVISOR'S NAME (Print Name)		17a. SUPERVISOR'S EMAIL ADDRESS
17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT		17d. SUPERVISOR SIGNATURE
18. INFORMATION OWNER/OPR PHONE NUMBER		18a. INFORMATION OWNER/OPR SIGNATURE
19. ISSO ORGANIZATION/DEPARTMENT		19b. ISSO OR APPOINTEE SIGNATURE
19a. PHONE NUMBER		19c. DATE (YYYYMMDD)
UNCLASSIFIED		
DD FORM 2875, MAY 2022		
PREVIOUS EDITION IS OBSOLETE		
Page 1 of 3		



MPAS – Change of Custody

- When transitioning from one MPAS to another, the new MPAS will need to be provisioned
 - See “Steps to Become an MPAS” slides above
- Once the new MPAS can successfully log into MP ICAM, the outgoing MPAS will email the MPASM team requesting a transfer of applicants while copying the new MPAS
- The MPASM team can transfer all applicants to the new MPAS
- It is the outgoing MPAS’ responsibility to ensure that this transfer is facilitated
- Lastly, the outgoing MPAS needs to request to the MPASM team to be removed from the site



Reverification

- Applicants must be reverified every 6 months
- If you don't see a Reverification button:
 - There are more than 59 days before reverification date
 - Sponsorship and/or contract end date is before the reverification date
 - Go to “Site Summary” > “Need Reverification” > sort by reverification date and on individual applicant records
 - Make sure sponsorship and contract end dates are in the future
 - Reverification button appears on Day 59