BY ORDER OF THE SECRETARY OF THE AIR FORCE, THE NAVY, HOMELAND SECURITY, COMMERCE, HEALTH AND HUMAN SERVICES

DEPARTMENT OF THE AIR FORCE INSTRUCTION 36-3026, VOLUME 2 BUPERS INSTRUCTION 1750.10D, MARINE CORPS ORDER (MCO) 5512.11F, COMMANDANT INSTRUCTION M5512.1B, NOAA CORPS DIRECTIVES, CHAPTER 1, PART 5

15 JANUARY 2026

Personnel

COMMON ACCESS CARD

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is 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: DAFI36-3026V2, 23 January 2023 | Pages: 72

This publication implements Department of the Air Force Policy Directive (DAFPD) 36-30 guidance for identification card issuing facilities supported by the Real-time Automated Personnel Identification System (RAPIDS) and the Defense Enrollment Eligibility Reporting System (DEERS). Volume 2 supports the ID card issuance lifecycle, including the administration of ID card benefits and privileges as listed in Department of the Air Force Instruction (DAFI) 36-3026, Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel.* This inter-service publication implements Department of Defense Manual (DoDM) 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* and Volume 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, DoD Instruction (DoDI) 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, DoDI 1000.25, *DoD Personnel Identity Protection (PIP) Program*, Federal Information Processing Standards Publication (FIPS) 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication 800-73-4, *Interfaces for Personal Identity Verification*; NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, Department of Commerce, NIST, Special

Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK)* Enabling, DoDI 1000.01, *Identification (ID) Cards Required by the Geneva Conventions*, DoDI 1341.02, *Defense Enrollment Eligibility Reporting System (DEERS) Programs and Procedures*, DoDI 1330.09, *Armed Services Exchange Policy*, DoDI 8500.01, *Cybersecurity*, and DoDI 8910.01, *Information Collection and Reporting*. Additionally, this inter-service publication supports the DEERS and the RAPIDS for the Navy (USN), Air Force (USAF), Space Force (USSF), Marine Corps (USMC), Coast Guard (USCG), the Commissioned Corps of the National Oceanic and Atmospheric Administration (NOAA), United States Public Health Service (USPHS), National Guard (ANG), and US Armed Forces and others that may be approved by the Undersecretary of Defense (Personnel and Readiness) (USD [P&R]). It supports policy and procedures for the issuance of Common Access Cards (CACs) to members of the Uniformed Services and DoD components (to include the National Guard, Selected Reserve, and Participating Individual Ready Reserve members in a training capacity), DoD Civilian employees, eligible non-DoD civilian employees of other Federal Agencies, State Employees of the National Guard, eligible contractor personnel, eligible foreign nationals (excluding foreign national contractor employees), contracted/enlisted Reserve Officer Training Corps cadets and midshipmen, and other eligible recipients as approved by USD (P&R). Use this publication to prepare issue, reissue, account for, and dispose of the CAC of the Uniformed Services, Department of Defense Components and other eligible recipients. This publication provides procedures for compliance of forms prescribed in the DoD RAPIDS Workstation and Verifying Official (VO) Certification Practice Statement, herein referred to as the RAPIDS/VO Certification Practice Statement. Compliance with attachments is mandatory. This publication implements DD Form 2841, *DoD Public Key Infrastructure (PKI) Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities*, DD Form 2842, *DoD Public Key Infrastructure (PKI) Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities*, DD Form 1172-2, *Application for Identification Card/DEERS Enrollment*, and DD Form 577, *Appointment/Termination Record-Authorized Signature*.

This publication implements Department of Air Force Policy Directive (DAFPD) 36-30, *Military Entitlements,* and is consistent with DoDI 1000.01, DoDI 1000.13, and DoDI 1341.02, *Defense Enrollment Eligibility Reporting System (DEERS) Program and Procedures*. This instruction applies to all civilian employees, uniformed members of the Regular Air Force (RegAF), the United States Space Force (USSF), the Air Force Reserve (AFR) and the Air National Guard (ANG) personnel, except where noted otherwise. This publication also includes instructions applying to Air Force RAPIDS facilities (RegAF, USSF, AFR, and ANG), identifying Tier waiver authorities (T-0, T-1, T-2, and T-3) as approved by the Air Force Inspector General Advisory Board.

Use this instruction to prepare issue, use, account for, and dispose of ID cards the Uniformed Services issue. The authorities to waive wing, unit, or delta level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAF Manual (DAFMAN) 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 Publication OPR for non-tiered compliance items. Waivers to this instruction are authorized and shall be processed IAW DAFMAN 90-161. Requests will be submitted using the DAF Form 679, *Department of the*

Air Force Publication/Form Action Request, or via e-mail or memorandum if the form is unavailable.

Vigilance must be taken to protect Personally Identifying Information when submitting or sending nominations, applications or other documents to DoD agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning. This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974, authorized by Department of Defense Instruction (DoDI) 5400.11, *DoD Privacy and Civil Liberties Program*. The applicable System of Record Notices Defense Manpower Data Center (DMDC), 02 DoD, Defense Enrollment Eligibility Reporting System (DEERS); available at **https://dpcld.defense.gov/Privacy/SORNs/**.

This publication is subject to the Paperwork Reduction Act of 1995. This publication may not be supplemented. Refer recommended changes and questions about this publication to AFPC/DP3SA using the DAF Form 847, *Recommendation for Change of Product.* Route DAF Forms 847 from the field through the appropriate functional chain of command. 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. DoD component services/organizations creating records as a result of this public must adhere to their service specific disposition schedule. Refer to **Attachment 1** for Glossary of References and Supporting Information. Compliance with attachments is mandatory.

SUMMARY OF CHANGES

This document has been revised to comply with Executive Order 14168, *Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government*.

Chapter 1—COMMON ACCESS CARD--GENERAL GUIDELINES 7

1.1. General Guidelines. 7
1.2. Identity Proofing and Vetting. 7
Table 1.1. Federal Investigative Standards (FIS). 7
1.3. Purpose of the Common Access Card. 8
1.4. Common Access Card Issuance Platform. 8
1.5. General Common Access Card Eligible Categories. 9
1.6. Types of Common Access Cards. 9
1.7. Expiration Dates. 9
Table 1.2. Common Access Card Type and Expiration Date Guidance. 9
1.8. Multiple Common Access Card 10
1.9. Reissuance. 10
1.10. Confiscating Common Access Cards 10

Table 1.3. Table 1.3.Individuals Who May Confiscate Common Access Cards. 10
1.11. Retrieval /Disposition of the Common Access Card. 11
1.12. Cross-Servicing Agreement for the Common Access Card..... 12
1.13. Temporary..... 12
1.14. Photograph Requirements for Common Access Card. 12
1.15. Copying Or Distribution Of Cards..... 12
1.16. Restrictions. 12
1.17. Color Coding..... 12
Table 1.4. Cardholder Color Coding Status. 13
1.18. Protective Sleeves. 13
1.19. Roles and Responsibilities. 13
Chapter 2—PERSONNEL ELIGIBLE FOR THE COMMON ACCESS CARD 14
2.1. Active, Selected Reserve, and National Guard. 14
2.2. Foreign Affiliate. 14
2.3. Civilian Affiliate. 14
2.4. Department of Defense/Uniform Services Employees. 15
2.5. Department of Defense or Uniformed Services Contractor Employees. 16
2.6. Identity Proofing and Registration. 17
2.7. New Members – Identity Vetting and Registration. 17
2.8. Central Issuing Facility. 18
2.9. Common Access Card Central Issuance Requesting Station. 18
2.10. Person-in-Charge. 18
Chapter 3—QUALIFYING REQUIREMENTS AND RESPONSIBILITIES FOR COMMON ACCESS CARD ISSUANCE 19
3.1. Qualifying Requirements. 19
3.2. Security Vetting Procedures. 20
3.3. Training Requirements. 20
3.4. Verifying Official/Issuing Official and Local Registration Authority. 20
3.5. Super Verifying Official. 21
3.6. Site Security Manager. 21
Chapter 4—REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM SITE MANAGEMENT 24
4.1. Cardstock Management. 24

4.2. Card Handling and Storage Guidelines. 24
4.3. Consumables: Printer Ribbon, Laminate, Cleaning Kit. 24
4.4. Equipment Relocation. 24
4.5. Continuity of Operations Plan. 25

Chapter 5—PERSONAL IDENTITY VERIFICATION PRIVACY REQUIREMENTS 26

5.1. Personal Identity Verification Requirements. 26
5.2. Personal Identity Verification – Federal Employees And Contractors. 26
5.3. Early Issuance. 26
5.4. Initial Issuance – Eligibility, Affiliation, Background Vetting, And Claimed Identity. 26
5.5. Replacement – Lost, Stolen, Printed Information Changed, And Card Media Damage. 27
5.6. Expiration Dates. 27
5.7. Common Access Card Public Key Infrastructure Certificates. 27
5.8. Multiple Common Access Card 28
5.9. Limited Off-line Issuance of Temporary Common Access Card. 28
5.10. Photograph Requirements. 28

Chapter 6—RAPIDS ASSISTANCE POINTS OF CONTACTS 30

6.1. Uniformed Services DEERS/RAPIDS Project Offices. 30
6.2. DEFENSE MANPOWER DATA CENTER SUPPORT HELPDESK: 31
6.3. DEFENSE MANPOWER DATA CENTER SUPPORT HELPDESK - DMDC SUPPORT CENTER-Asia (DSC-A). 31
6.4. DEFENSE MANPOWER DATA CENTER SUPPORT CENTER-Europe (DSC-E): 31
6.5. Social Security Administration. 32

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 33

Attachment 2—COMMON ACCESS CARD ENTITLEMENT TABLES 45

Attachment 3—BASIC DOCUMENTATION OR ACCEPTABLE INFORMATION SOURCES FOR SPONSORHIP IN DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM 46

Attachment 4—DEPARTMENT OF DEFENSE LIST OF ACCEPTABLE IDENTITY DOCUMENTS 49

Attachment 5—INSTRUCTIONS FOR COMPLETION OF DD FORM 1172-2, “APPLICATION FOR IDENTIFICATION CARD/DEFENSE

ENROLLMENT ELIGIBILITY REPORTING SYSTEM ENROLLMENT" 50

Attachment 6—SAMPLE SIGNATURE AUTHORIZATION LETTER AND DD FORM 577, "APPOINTMENT/TERMINATON RECORD – AUTHORIZED SIGNATURE" 63

Attachment 7—DD FORM 2841, "DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES" 64

Attachment 8—DD FORM 2842, DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES (SUBSCRIBER) 65

Attachment 9—RETURNING COMMON ACCESS CARD TO DEFENSE MANPOWER DATA CENTER SUPPORT CENTER 66

Attachment 10—REAL TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM (RAPIDS) SITE SECURITY MANAGER (SSM)/VERIFYING OFFICIAL(VO)/ ISSUING OFFICIAL (IO) PROCEDURES FOR LOST, STOLEN, OR DESTROYED IDENTIFY CREDENTIAL – COMMON ACCESS CARD 67

Attachment 11—SAMPLE MEMORANDUM LOST, STOLEN, DESTROYED IDENTITY CREDENTIAL – COMMON ACCESS CARD 68

Attachment 12—MISSION PARTNER IDENTITY, CREDENTIALING AND ACCESS MANAGEMENT, DEFENSE BIOMETRIC IDENTIFICATION SYSTEM, DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (DBIDS), DEFENSE NATIONAL VISITOR CENTER, DEFENSE CROSS-CREDENTIALING IDENTIFICATION SYSTEM, REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM SELF-SERVICE (RSS), AND COMMON ACCESS CARD PERSONAL IDENTITIFICATION NUMBER RESET PROGRAMS, VOLUNTEER LOGICAL ACCESS CREDENTIAL, MILCONNECT, ID CARD OFFICE ONLINE, NIPRNET ENTERPRISE ALTERNATIVE TOKEN SYSTEM PROGRAMS 70

Chapter 1

COMMON ACCESS CARD--GENERAL GUIDELINES

1.1. General Guidelines. The Department of Defense (DoD) Common Access Card (CAC) meets the Federal requirements for credentialing contained within Homeland Security Presidential Directive-12 and FIPS Publication 201-3. Refer to DoDI 1000.13, January 23, 2014, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,* DoDM 1000.13, Volume 1, January 23, 2014, *DoD Identification Cards*: ID Card Life-Cycle DoDM 1000.13, Volume 2, January 23, 2014, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,* and 32 CFR, Part 161, Federal Register/Volume 81, Number 208, October 27, 2016 – Identification (ID) Cards for Member of the Uniformed Services, Their Dependents, and Other Eligible Individuals.

1.1.1. This inter-service instruction applies to all eligible CAC populations, DoD, the Military Departments (including the Coast Guard (USCG) at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), and all other Federal agency and organizational entities associated with the DoD.

1.1.2. This inter-service instruction also applies to the Commissioned Corps of the US Public Health Service (USPHS), under agreement with the Department of Health and Human Services, and the National Oceanic and Atmospheric Administration (NOAA), under agreement with the Department of Commerce.

1.1.3. All uniformed Services Real-time Automated Personnel Identification System (RAPIDS) sites are required to maintain a printed copy of this inter-service instruction DAFI 36-3026, Volume 2 in case of emergencies as well as for informational and training purposes according to **paragraph 1.12**., Cross-Servicing Agreement. **(T-3)**

1.2. Identity Proofing and Vetting.

1.2.1. CAC eligible individuals will not be issued a CAC without first satisfying the background vetting requirements in accordance with Homeland Security Presidential Directive-12, and Office of Management and Budget M-05-24, *Implementation of Homeland Security Presidential Directive* 12-Policy for a Common ID Standard for Federal Employees and Contractors. **(T-1)** Initial issuance of a CAC requires, at a minimum, the completion of a Federal Bureau of Investigation fingerprint check with favorable results and submission of a National Agency Check with Inquiries to the Office of Personnel Management, Defense Counterintelligence and Security Agency, or a DoD-determined equivalent investigation. **Table 1.1** below outlines an authoritative list of background investigation for Personal Identity Verification, including those approved by OUSD(I) as being equivalent to (or greater than) National Agency Check with Inquiries.

Table 1.1. Federal Investigative Standards (FIS).

Tier	Investigation Type	Description
1	(NACI) -National Agency Check plus Written Inquires and Credit Check.	Low Risk, Non-Sensitive, includes HSPD-12 credentialing.
2	(MBI) - Minimum Background Investigation.	Moderate Risk Public Trust (MRPT).

3	(NACLC) - National Agency Check, Local Agency Check & Credit Check. (ANACI) – Access National Agency Check with Written Inquiries & Credit Check.	Non-Critical Sensitive National Security, including Secret and "L" access eligibility or access to Confidential or Secret information.
4	(BI) - Background Investigation	High Risk Public Trust (HRPT).
5	(SSBI) - Special Background Investigation plus Current Background Investigation	Critical Sensitive and Special Sensitive National Security, including Top Secret, SCI, and "Q" access eligibility.

1.2.2. ID cards must be issued to the CAC holder in person. **(T-0) Exception**: Cards generated by a Central Issuance Facility may be issued and distributed by the Person in Charge.

1.2.3. Identity Verification. During the CAC issuance process, all personnel shall present two forms of ID in original form to verify a claimed identity. **(T-2)** The identity source documents must come from the DoD List of Acceptable Identity Documents for identity proofing, DEERS enrollment, eligibility, and ID card issuance purposes (see **Attachment 4**). **(T-2) Note:** Defense Enrollment Eligibility consistent with the DoD List of Acceptable Identity Documents at least one document from the **Attachment 4** shall be a valid (unexpired) State or Federal Government-issued picture identification. **(T-0)** The identity documents will be inspected for authenticity and scanned and stored in the DEERS to the RAPIDS User Guide upon issuance of an identification. **(T-0)** The photo identification requirement cannot be waived, consistent with applicable statutory requirements. **(T-0)**

1.2.4. In the future, RAPIDS sites will have the capability to verify the background vetting processes have been initiated and/or successfully completed from DoD or from a Federal Government authoritative data source. Once this capability is in place, any CAC applicant who is identified in RAPIDS as not meeting the required vetting requirements will be directed to his or her local human resource offices, personnel security offices, or Government sponsor to initiate the vetting process or verify that the vetting has been completed. **(T-3)**

1.3. Purpose of the Common Access Card. The CAC is the ID card used as a primary physical and logical access token for the DoD for uniformed Services personnel, to include Active Component, Selected Reserve, Participating Individual Ready Reserve, Armed Forces Health Professions Financial Assistance Program, Reserve Officer Training Corps cadets and other eligible populations as referenced in **paragraph 1.1.2.**, USCG civilian employees, eligible non-Department of Defense civilian employees of other Federal Agencies, State Employees of the National Guard, eligible contractor personnel (refer to Terms), and other eligible recipients as approved by USD (P&R). The CAC will be used for physical access to buildings, facilities, installations, and controlled spaces; serves as a primary platform for the public key infrastructure authentication token in the unclassified environment used to access the Department's computer networks and systems. **(T-0)** The CAC also will be used to facilitate standardized, uniform access to DoD facilities, installations, and computer systems. **(T-0) Note:** For those individuals not eligible for a CAC but requiring physical access to local or regional areas (e.g., retired military, family members and certain contractors) an alternative non- Homeland Security Presidential Directive-12 compliant card will be issued. **(T-3)** This population, if eligible, will continue to use DoD ID cards pursuant to DoDI 1000.13 Volume 1, Enclosure 2, until they are migrated to an applicable new card (refer to **Chapter 2** within this instruction). **(T-3)**

1.4. Common Access Card Issuance Platform. The CAC is generated by the RAPIDS, an application of the DEERS.

1.4.1. Authoritative Data Source. According to USD (P&R) Memorandum, *DEERS/RAPIDS Lock Down for Contractors,* November 10, 2005, *DEERS/RAPIDS Lock Down for Additional Populations,* October, 29, 2010, and memorandums codified in DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* January 23, 2014 CAC eligible personnel must be registered in DEERS through either an authoritative personnel data feed from the appropriate Service or Agency, or through the Mission Partner (MP) Identity, Credentialing and Access Management (ICAM) formerly Trusted Associate Sponsorship System (TASS).

1.4.2. The CAC surface shall not be amended, modified, or overprinted by any means. **(T-0)** No stickers or other adhesive materials shall be placed on either side of the CAC. **(T-0)** No holes shall be punched into the CAC. **(T-0)** The chip or laminate shall not be removed; doing so would be considered defacing the CAC. **(T-0)** Defacing the CAC will affect the validity of the CAC and the card applications**. (T-0)**

1.4.3. The CAC, when worn is on the front of a body, displayed above the waist and below the neck in accordance with Agency/Service specific instructions.

1.5. General Common Access Card Eligible Categories. Refer to DoDM 1000.13, Volume 1 and **paragraph 1.4**. Surviving Family Members--upon request, next of kin may obtain the CAC for an individual who has perished in the line of duty. All CACs provided to next of kin must be terminated, have the certificates revoked, and have a hole punched through the Integrate Circuit Chip prior to release. **(T-1)**

1.6. Types of Common Access Cards. There are four CAC types used within the Department, based on cardholder eligibility. Refer to DoD website **www.cac.mil** for card type examples.

1.7. Expiration Dates. The CAC shall be issued for no more than three years, or to the end of the cardholder's term of service, contract, employment, or association with the DoD, whichever is earlier. **(T-1)** Services Academies will issue a 4-year CAC with a 3-year Public Key Infrastructure (PKI) certificate. **(T-1)** For contractors, CACs will be issued for three years or the duration of the contract, not to exceed a 3-year time period per the MP-ICAM (formerly TASS), enrollment transaction to DEERS. **(T-1)** See **paragraph 1.10** for individuals who may confiscate CACs.

Table 1.2. Common Access Card Type and Expiration Date Guidance.

Common Access Card Type	Expiration Date
Armed Forces of the United States Geneva Conventions Identification Card	The earliest of three years, the date of expiration of term of active service, expiration of enlistment contract. **Exception:** Expected date of graduation from pre-commissioning programs, e.g., service academies, Officer Cadet School, Officer Cadet Candidate, Officer Training School.
United States DoD/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces	The earliest of three years, or the expected termination of cardholder's employment or association with the DoD or Uniformed Services, Emergency Essential status,

	contingency contractor status, or length of deployment.
United States DoD/Uniformed Services Identification Card	The earliest of three years or expected termination of the recipient's employment or association with the DoD or upon termination of the entitlement condition. See **Attachment 2**, including termination of benefits & privileges when authorized according to this instruction and DAFI 36-3026, Volume 1.
United States DoD/Uniformed Services Identification and Privilege Card	

1.8. Multiple Common Access Card Issuance. Individuals who are eligible for the CAC shall receive a separate CAC in each category for which they qualify, (e.g., a Reservist who is a DoD contractor employee). **(T-0) Note:** Only the CAC that is appropriate for access to a specific network and/or facility is issued for each category for which the individual qualifies.

1.9. Reissuance. The CAC shall be replaced upon expiration, when lost or stolen, when printed information has changed, or when any of the media (to include printed data, magnetic stripe, either of the bar codes, or the chip) becomes illegible or inoperable. **(T-1) Note:** Individuals are allowed to apply for a CAC renewal starting 90 days prior to their expiration of a valid identification.

1.9.1. Reissue CAC in accordance with DAFI 36-3026, Volume I, Chapter 9 for members being processed for administrative or judicial action, members court-martialed, placed in civilian or military confinement, or placed on appellate review leave.

1.9.2. Initial Issue and Reissue. Provide and explain to the CAC recipient that their signature on the DD Form 2842, *DoD Public Key Infrastructure (PKI) Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities*, acknowledges reading and accepting their responsibilities and obligations as stated on the form (see **Attachment 8**) Refer to DAFI 36-3026, Volume 1, Chapters 12, 13, 15, 17, 18, and Service unique requirements.

1.10. Confiscating Common Access Cards. CACs are property of the US Government. When a CAC has expired, is being fraudulently used, is mutilated, illegible, or is presented by a person not entitled to its use, the individuals listed in **Table 1.3** may confiscate CACs under the following conditions:

Table 1.3. Individuals Who May Confiscate Common Access Cards.

WHO CONFISCATES CACs	CONDITION
Verifying Officials, commissioned or noncommissioned officers, military police members, or base entry controllers.	A CAC has expired. A CAC is being fraudulently used. A CAC is presented by a person not entitled to its use. A CAC is mutilated or illegible.
Senior Installation Officials.	Shoplifting is involved. The Senior installation official determines when to confiscate CAC. Senior installation officials, installation security authorities and installation legal staffs establish written base policy for confiscating

	CAC when shoplifting has occurred. (See **Attachment 1**, Definitions.)
Civilian Employees, including Human Resource administration and supervisors (appropriated and Non-appropriated funds) activities). **Note**: Individuals who are employed in facilities that provide benefits and privileges: exchange/ commissary identification card checkers, medical providers, Morale, Welfare, and Recreation and customer services representatives, etc.	CAC recipients of any Service have cards that are mutilated so that their use as a CAC is questionable. The CAC has expired, altered, or an ineligible person.

1.10.1. Notify the installation security authorities immediately after having confiscated a CAC or if involved in a situation requiring confiscation of a CAC.

1.10.2. Installation security authorities investigate confiscation cases or refer these cases to the appropriate Service special agent office (see **Attachment 1**, Definitions) when it is warranted by circumstances or according to local procedures.

1.10.3. Installation security authorities provide the parent Service all information pertaining to the situation when the confiscated card belongs to a member of another Service.

1.10.4. Give a receipt or letter to the cardholder when confiscating a CAC.

1.10.5. Return confiscated CACs immediately to the nearest RAPIDS site with the reason for confiscation.

1.11. Retrieval /Disposition of the Common Access Card. CACs confiscated or turned in as invalid, inaccurate, inoperative, or expired shall be returned to a RAPIDS site for disposition in accordance with **Attachment 9** of this instruction and the RAPIDS User Guide. **(T-0)**

1.11.1. The CAC is the property of the US Government and shall be in the personal custody of the member at all times. **(T-1)** Upon termination of employment, retirement or death, the CAC must be recovered. **(T-0) Note:** All recoverable CACs will be returned to DMDC for accountability from the RAPIDS facility. **(T-1) Exception:** Upon request, next of kin may obtain the CAC for an individual who has perished in the line of duty. All CACs provided to next of kin must be terminated, have the certificates revoked, and have a hole punched through the Integrate Circuit Chip prior to release. **(T-0)**

1.11.2. CAC-eligible populations will follow local in/out-processing procedures that include revoking the CAC certificates for inter-departmental employment changes, relocations, etc. **(T-3)** This also includes updating the PKI email encryption and digital signature. Individuals being transferred within the Department, including mobilization must ensure their DEERS records pertaining to the CAC are updated to DEERS. **(T-3)** This record action is accomplished by the appropriate Service/Agency to DEERS. **Note:** Civilian personnel of the DoD who are transferring between components (e.g., a civilian employee of the ARMY takes a new job as civilian employee with the AF), will be permitted to retain their CAC to allow the person to have an operational CAC and be fully capable on their first day of work.

1.12. Cross-Servicing Agreement for the Common Access Card. RAPIDS site shall, on presentation of the required documentation, sponsorship, or verification through DEERS, issue a CAC to any eligible recipient. **(T-3)** Initial issue and renewal of a CAC for contractor employees requires coordination of the sponsoring service contracting official with the intended issuing facility through the MP-ICAM (formerly TASS) see **Attachment 12**.

1.12.1. The DD Form 577 is the signature card, or a signature memorandum is an administrative process, allowing the Contracting Officer or government official to sign the DD Form 1172-2 authorizing issuance of the CAC to a person upon meeting the qualifications according to DoDM 1000.13, Volume 1. See DD Form 577 at **Attachment 6** or sample signature memorandum at **Attachment 5**. **Note**: the MP-ICAM (formerly the TASS), the DD Form 577, signature memorandums, or DD Form 1172-2 will no longer be required for contractor personnel DEERS enrollment, with the limited exception of Foreign Affiliate and National personnel.

1.12.2. DoD contractor personnel are not authorized to sign the DD Form 577 or signature memorandum. This verification process can only be accomplished by the Contracting Officer Representative, Quality Assurance Evaluator, Contracting Officer Technical Representative, the designated CO assigned to the installation contracting office, or the installation's designated representative.

1.13. Temporary Common Access Card. If a member has been mobilized and there are no communications either with the DEERS database or the CA, a temporary card can be issued with an abbreviated expiration date for a maximum of 10 days. The temporary card will not have PKI certificates and will be updated as soon as the member can reach an online RAPIDS station or communications have been restored. **(T-1)** This also applies to military being mobilized or civilians and contractors receiving Geneva Convention Cards. The temporary card will appear the same as the Armed Forces of the United States Geneva Conventions Identification Card with a white space where the chip is normally located. **(T-1)**

1.14. Photograph Requirements for Common Access Card. (**See paragraph 5.10**.).

1.15. Copying Or Distribution Of Cards. Section 701 of Title 18, United States Code prohibits photocopying or other reproduction of DoD ID cards except by regulation. When possible, the card will be electronically authenticated in lieu of photographing the card. **(T-3) Note:** The cardholder may allow photocopying of their identification card to facilitate DoD benefits, e.g., processing medical claims.

1.16. Restrictions. There are instances where graphical representations of CACs are necessary to facilitate the DoD mission. When used or distributed, these graphical representations must not be the same size as the CAC and must have the word "SAMPLE" written on them. **(T-0) Note:** Sample identification cards, not the actual size, with the word 'EXAMPLE" or "SAMPLE" printed across the card may be posted on a PKI enabled web sites, however, they shall not be posted on public websites. **(T-0)**

1.17. Color Coding. The CAC shall be color coded as indicated below to reflect the status of the cardholder (see **Table 1.4**). **(T-0)**

Table 1.4. Cardholder Color Coding Status.

No Color Stripe **"W" White**	US military and DoD civilian personnel or any personnel eligible for a Geneva Conventions card
Blue Color Stripe **(formerly red stripe)** **"B" Blue**	Non-US personnel, including DoD contract employees (other than those persons requiring a Geneva Conventions card)
Green Color Stripe **"G" Green**	All personnel under contract to the DoD (other than those persons requiring a Geneva Conventions card)
Red Color Stripe **"R" Red**	Reserved for First Responder personnel.
Note: The First Responder card is pending migration to the DEERS/RAPIDS platform.	

1.17.1. If a person falls into multiple categories, meeting more than one condition above, priority is given to the blue stripe to denote a non-US citizen, unless the card serves as a Geneva Conventions card.

1.17.2. FIPS 201-3 reserves the red color stripe to distinguish emergency first responder officials.

1.18. Protective Sleeves. Electromagnetically opaque sleeves or other comparable technologies are the requirement of DoD Components to protect against any unauthorized contactless access to the cardholder unique identification number stored on the CAC in accordance with Federal Information Processing Standards - 201. Products certified to meet this requirement are listed on the General Services Administration products list (**https://www.idmanagement.gov/**) approved by Federal Information Processing Standards 201. DoD Components should consider their different environmental and operational considerations in addressing which type of opaque sleeves will meet their mission's needs.

1.19. Roles and Responsibilities. Uniformed Services DEERS Project Offices and RAPIDS issuing sites will implement DEERS enrollment and eligibility policy guidance and procedures relating to identification card eligibility and issuance, including benefit entitlement eligibility impacting DEERS populations. **(T-0)** Uniformed Services DEERS Project Offices responsibilities include implementing guidance and procedures to support RAPIDS issuing site tasks. Refer to DAFI 36-3026, Volume 1, paragraph 1.5, Verifying Official Responsibilities and Chapter 10, RAPIDS and DEERS Procedures.

Chapter 2

PERSONNEL ELIGIBLE FOR THE COMMON ACCESS CARD

2.1. Active, Selected Reserve, and National Guard. The DoD provides CACs to members of the DoD and military components, DoD contractors including members and contractor populations of the NOAA and the USPHS, and USCG, non-DoD Federal civilians, state employees, and other non-DoD affiliates. The CAC identifies the recipient's benefits and privileges (if applicable) to the Uniformed Services and will be used for physical access to buildings, facilities, installations, and controlled spaces; will serve as the primary platform for a public key infrastructure authentication token in the unclassified environment where it will be used to access the department's computer networks and systems. **(T-1)** It also serves as the Geneva Conventions Identification Card. **Note:** See **Attachment 2** for eligible benefits and **Attachment 3** for Basic Documentation or Acceptable Information Sources Required to Determine/Verify Eligibility for Enrollment or Issuance of CAC.

2.1.1. Members of the NOAA and the USPHS CACs shall reflect Uniformed Services. **(T-1)**

2.1.2. Reservists on active duty or ANG members on full-time ANG duty for 31 days or more will update information on the chip to reflect current military status. **(T-1)**

2.2. Foreign Affiliate. Non-US Citizen Sponsors and their Dependents, Foreign Affiliate (formerly foreign military) personnel, and International Military Students (IMS) are issued the United States DoD/Uniformed Services Identification (USID) when qualifying for DoD benefits and privileges according to DoDM 1000.13, Volume 2.

2.2.1. Foreign personnel will have the US equivalent rank as determined by the sponsoring agency, printed on the USID or CAC. CAC issuance must follow Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12. CAC issuance occurs when a Foreign Affiliate has an approved application from MP-ICAM sent to DEERS by the Mission Partner Affiliation Sponsor (MPAS) (**T-1**) **Note:** See **Attachment 2** for eligible benefits and **Attachment 3** for Basic Documentation or Acceptable Information Sources Required to Determine/Verify Eligibility for Enrollment or Issuance of CAC. The CAC will reflect the equivalent rank according to the DEERS/RAPIDS application. **(T-1)** The DoD/Uniformed Service sponsoring agency should validate the rank equivalent and include it on official documentation, i.e., the DD-Form 1172-2, memorandum, or travel order at card issuance, replacement, or update.

2.2.2. IMS attending education or training in the US. Effective 22 September 2022, RAPIDS software issues the USID to IMS personnel. USID reflects benefits and privileges for the IMS and accompanying dependent family members when they are authorized by International Travel Order (ITO). Refer to DAFI 36-3026 Vol 1, Attachment 5 and Table A5.1, for determining DEERS eligibility. Acceptable documents to determine DEERS eligibility are ITO, Foreign Visit Request (FVR), and Extended Visit Authorization (EVA).

2.3. Civilian Affiliate. CAC eligibility for DoD contractors, non-DoD Federal civilians, State employees, and other non-DoD affiliates is based on the government sponsor's determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission. **(T-3)** Individuals qualifying for a PIV credential according to DoDM 1000.13,

Volume 1, CAC issuance occurs when a civilian affiliate has an approved application from MP-ICAM sent to DEERS by the MPAS.

2.4. Department of Defense/Uniform Services Employees. DoD civilian employees are eligible for one of three CAC types contingent on meeting the respective qualifying criteria as described in the following paragraphs. The latter two are issued based on specific qualifying criteria in addition to physical and systems access. The criteria include those who, based on their assignment location, qualify for an identification card, or an identification card authorizing privileges; and those who qualify for an identification card (requiring Geneva Conventions identification) and privileges. For qualifying source documents see **Table A3.2**. Refer to DAFI 36-3026, Volume 1, for General Schedule Equivalency scale rating. **Note:** See **Attachment 2** for eligible benefits (when qualifying) and **Attachment 3** for Basic Documentation or Acceptable Information Sources Required to Determine/Verify Eligibility for Enrollment or Issuance of CAC.

2.4.1. The United States DoD/USID Card is issued to DoD civilian employees including NOAA, USPHS, and USCG in the following categories:

2.4.1.1. Civilian employees (see Terms) to include:

2.4.1.1.1. Individuals appointed to appropriated fund and non-appropriated fund positions.

2.4.1.1.2. Permanent or time-limited employees on full-time, part-time, or intermittent work schedules. **Note:** There is no minimum time of employment required for CAC issuance.

2.4.1.1.3. Senior Executive Service, competitive service, and Excepted Service employees.

2.4.1.1.4. Non-US citizens employed by or under the sponsorship of DoD.

2.4.1.2. Civilian employees who operate RAPIDS workstations at Federal Agencies, other than DoD (e.g., NOAA, USPHS, USCG).

2.4.1.3. Civilian employees of other Federal agencies who require access to DoD networks to perform their duties.

2.4.1.4. State employees of the ANG.

2.4.1.5. Other civilian categories as determined by USD (P&R).

2.4.2. The United States DoD/USID and Privilege Card is issued to CAC – eligible civilian employees who are: See **Attachment 2** for eligible benefits.

2.4.2.1. Required to reside in a household on a military installation within the continental United States, Hawaii, and Alaska.

2.4.2.2. Required to reside in a household on a military installation, hired under a transportation agreement or employed by the Uniformed Services or DoD in Puerto Rico and Guam. Entitlements and privileges vary. See **Attachment 2**.

2.4.2.3. Stationed or employed and residing in foreign countries for a period of 365 days or more. Individuals who perform overseas temporary duties (less than 365 days) are not eligible for issuance of the CAC identification and Privilege card.

2.4.2.4. DoD Presidential Appointees who have been appointed with the advice and consent of the Senate. These appointees are authorized medical and emergency dental care in military medical and/or dental treatment facilities within the continental United States. Within the National Capital Region, charges for outpatient care are waived. Charges for inpatient and/or outpatient care provided outside the National Capital Region will be at the interagency rates. **(T-1)**

2.4.2.5. Civilian employees of the Army and Air Force Exchange Service, Navy Exchange System, Marine Corps Exchange System, and USCG. Exchange employees are entitled to all privileges of the exchange system, except for purchase of articles of uniform and state tax-free items.

2.4.3. The United States DoD/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces is issued to CAC eligible civilian employees who are:

2.4.3.1. Emergency-Essential employees. Emergency-Essential employees as defined in DTM-17-004 who are assigned in an EE civilian position and required to sign the DD Form 2365, *DoD Civilian Employee Overseas Emergency-Essential Position Agreement*.

2.4.3.2. Civilian noncombatant personnel who have been authorized to accompany military forces of the United States in regions of conflict, combat, and contingency operations and who are liable to capture and detention by the enemy as prisoners of war.

2.5. Department of Defense or Uniformed Services Contractor Employees. Contractor employees can qualify for one of three CAC types depending on respective qualifying criteria. Refer to **Attachment 2** for entitlements because medical benefits and shopping privileges vary. **Note:** A personnel data feed from the MP-ICAM, (formerly TASS) to DEERS must occur before a CAC can be issued from RAPIDS. Refer to DoD Contractor Personnel Office for contractors employed in Germany and Italy.

2.5.1. The United States DoD/USID Card identity credential is issued to eligible contractor employees who are under the terms and conditions of a DoD, Uniformed Services, NOAA, or USPHS contract. Contractor employees are required to have physical access to buildings, facilities, installations, and controlled spaces, or access to DoD or Uniformed Services identification computer networks and systems. **Note:** See **Attachment 2** for eligible benefits and **Attachment 3** for Basic Documentation or Acceptable Information Sources Required to Determine/Verify Eligibility for Enrollment or Issuance of CAC.

2.5.2. The United States DoD/USID and Privilege Card identity and privilege credential is issued to contractor employees (see **Attachment 2**) for eligible benefits who are:

2.5.2.1. Required to reside in a household on a military installation within the continental United States, Alaska, and Hawaii. **Note:** Alaska and Hawaii are not considered overseas locations for the purpose of CAC entitlements. See **Attachment 2**.

2.5.2.2. Required to reside in a household on a military installation, hired under a transportation agreement or employed by the Uniformed Services or DoD within Puerto Rico and Guam. Entitlements to medical benefits and shopping privileges vary. See **Attachment 2**.

2.5.2.3. Stationed or employed and residing in foreign countries for a period of at least 365 days or more. **Note:** Contractor employees who perform frequent overseas temporary duties are eligible for the Identity CAC only and are not eligible for issuance of the CAC Identification and Privilege card for temporary duty periods less than 365 days.

2.5.2.4. Other federal agencies employing individuals under separate contract, referred to as "Other Federal Agency Contractor" and not under contract with DoD are ineligible for the CAC, example, Department of Energy contractor employee. **Note:** Other Government agency contractors permanently assigned overseas refer to DAFI 36-3026, Volume 1, Attachment 2. If not assigned overseas, issuance of the DD Form 2765, reflecting shopping privileges is not authorized.

2.5.3. The United States DoD/USID Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces is issued to CAC eligible contractor employees who are: Refer to DAFI 36-3026, Volume I, Attachment 13 for General Schedule Equivalency scale rating.

2.5.3.1. Designated as a contingency contractor as stipulated within the contract. See **Attachment 1** for terms. The Synchronized Pre-deployment and Operational Tracker will be used by the contracting community for categorizing contractor personnel who are traveling to contingency operation locations. **(T-3)** Synchronized Pre-deployment Operational Tracker digitally signs the Letter of Authorization with the barcode and shall be the only accepted form for contractor personnel deploying for 30 days or more to receive a CAC. **(T-1)**

2.6. Identity Proofing and Registration. The Federal Information Processing Standards – 201, sets forth minimum criteria for vetting individuals seeking Federal employment or those seeking access to Federally controlled physical facilities or information resources, such as civilian and contractor personnel.

2.7. New Members – Identity Vetting and Registration. The following information is provided concerning identity source document inspections and background investigations. This process is conducted during the initial identity registration and prior to CAC issuance at a RAPIDS facility. **Note:** There are separations of duties and responsibilities in the CAC credential registration for enrollment and issuance process. This prevents a single individual from issuing a card without the participation of another authorized person to perform enrollment for DEERS. **(T-0)**

2.7.1. The initial registration process may be performed by the MP-ICAM (formerly TASS), Military and Civilian Personnel Data Systems provide authoritative data feed to DEERS; however, the registration of new members and their identity source document and background investigations shall be followed up on to authenticate a claimed identity prior to DEERS enrollment and CAC issuance. **(T-1)**

2.7.2. Individual shall appear in person and provide two forms of identity source documents in original form to the Verifying Official (VO). **(T-0)**

2.7.3. The identity source documents must come from the lists of acceptable documents included in US Citizenship and Immigration Services, Form I-9, Office of Management and Budget No. 1115-0136, "*Employment Eligibility Verification.*" **Note:** At least one document shall be a valid unexpired State or Federal government-issued picture identification. **(T-1)**

2.7.3.1. The VO shall visually inspect the identification documents and verify the document as being genuine and unaltered. **(T-1)**

2.8. Central Issuing Facility. Supports the Common Access Card Central Issuance Requesting Station (CACCIRS) at high-volume RAPIDS military academies and training centers. **Note:** The Central Issuing Facility (CIF) location is off-site from the CACCIRS and supports the following:

2.8.1. Mass Issuance. Production of a fully functional and personalized CAC with option to inject:

2.8.1.1. All PKI and Personal Identity Verification (PIV) certificates,

2.8.1.2. Identity certificate only, or

2.8.1.3. No PKI certificates (chip-less)

2.8.2. Mass issuance of CAC to all Uniformed Services cadets/recruits/trainees: active, guard, and reserve members; reduces RAPIDS data collection to meet Services training schedules. **Note**: There are no current requirements to issue to other personnel categories, i.e., military dependents, retirees, or other CAC eligible populations.

2.9. Common Access Card Central Issuance Requesting Station. DMDC Program Management Review initiative implemented the CACCIRS at Uniformed Services sites with large transient populations, i.e., training centers and Service Academies. CACCIRS converts USID card operations to a CAC enabled PKI environment for physical access to buildings and computer networks and serves as an identification card to meet Homeland Security Presidential Directive-12 criteria.

2.10. Person-in-Charge. The Person in Charge or Site Security Manager (SSM) at the CACCIRS site location will have telephone and email access to the Central Issuing Facility manager, Seaside, CA. The Central Issuing Facility manager will monitor all incoming/outgoing batch shipments with notices going to Service Project Office. **(T-3) Note:** Batch shipments not received/acknowledged by the Person in Charge or SSM, i.e., lost/stolen are reported according to protocol as established by the Central Issuing Facility manager and Service Project Office.

2.10.1. A minimum of two SSM or Person in Charge with alternate back-up personnel are required to secure separate shipments of CAC and Personal Identification Numbers (PIN)s. The Person in Charge/Site Security Manager will:

2.10.2. Monitor and acknowledge the shipment activity for CAC and PIN receipts through the web based Inventory Logistics Portal. **(T-1)** Refer to the Inventory Logistics Portal User Guide for card stock and consumable information.

2.10.3. Comply with PKI/Local Registration Authority (LRA) VO Certification Practice Statement responsibilities. **(T-1)**

Chapter 3

QUALIFYING REQUIREMENTS AND RESPONSIBILITIES FOR COMMON ACCESS CARD ISSUANCE

3.1. Qualifying Requirements. DEERS/RAPIDS operators, a minimum of two SSM and a minimum of one Super VO. The SSM and Super VO can be the same person performing both roles, including the role of Verifying/Issuing Official (IO), LRA. The Super VO also has the ability to access RAPIDS reports from the QLIK web application. DEERS/RAPIDS operators must be US citizens in order to issue PKI certificates in accordance with DoDI 8500.01. **(T-0)** **Note:** Local National and Military Affiliate (foreign national/civilian or military) are not authorized to operate RAPIDS in accordance with the RAPIDS Security Standard Operating Procedure 7.1. In addition, RAPIDS operators are prohibited from becoming a Trusted Agent Security Manager or Trusted Agent for the MP-ICAM, (formerly TASS). Likewise, Trusted Agent Security Managers and Trusted Agents are not authorized to become RAPIDS operators as SSM or VO.

3.1.1. Local commanders, agency department heads, or their authorized designees shall assign individuals to serve as SSM, Super VO, VO/IOs/LRA following the Grade Authorization for CAC Issuing/VO/LRA Officials in **Attachment 1**, Definitions, IO/VO/LRA Official. **(T-3)** Access to RAPIDS, (e.g., workstation, deployable, shipboard, and Central Issuing Facility) are restricted to users who are in compliance with the security requirements outlined in the DoD Personnel Security Regulation, DoDM (DoDM) 5200.2, *Procedures for the DoD Personnel Security Program (PSP)* and x.509 Certificate Policy for the United States DoD. **Note:** All RAPIDS users are considered Certificate Management Authorities. See DoDM 5200.2 Information Technology (IT-II) position category and related duties.

3.1.2. Security Requirements. Military members, DoD Civilian employees and contractor personnel must all meet the security requirements as indicated below. **(T-0)** Personnel must:

3.1.2.1. Have an IT-II security investigation per DoD 5200.2R, a positive result from Federal Bureau of Investigation fingerprint check, and an initiated National Agency Check with Inquiries or equivalent prior to receiving logon access to D/R. **Note:** SSM must have a favorable National Agency Check with Inquiries or Office of Personnel Management Tier 1 standards (refer to Office of Personnel Management security investigation check). **(T-0)**

3.1.2.2. Be a US citizen who serving in the US military, employed as DoD civilian, or employed as a DoD contractor requiring a National Agency Check with Inquiries or equivalent which includes the Federal Bureau of Investigation 10-fingerprint check. **(T-0)**

3.1.2.3. Have never been relieved of Certification Authority, Registration Authority, LRA, DEERS roles or Communication Security custodian duties for reasons of negligence or non-performance of duties. **(T-0)**

3.1.2.4. Have never been denied a security clearance or had a security clearance revoked. **(T-0)**

3.1.2.5. Have never been convicted of a felony offense. **(T-0)**

3.2. Security Vetting Procedures.

3.2.1. The SSM will verify that proper background vetting has been completed before logon access will be granted to the VO, IO, or LRA. **(T-1)**

3.2.2. The Service/Agency D/R Project Office will verify that the proper background vetting has been completed before logon access will be granted to the SSM by the DMDC/PIPS. **(T-1)**

3.3. Training Requirements. All personnel receiving access to D/R will require training and certification through the Defense Manpower Data Center (DMDC) Learning Management System. **(T-0)** Additional information can be found at the following website at **https://dhra.deps.mil/sites/dmdc/status/vois/SitePages.aspx**.

3.3.1. The VO/LRA shall be trained on the secure operations of RAPIDS to include printing and encoding a CAC and maintenance of equipment. **(T-0)** DMDC Access Card Office provides web-based training for all RAPIDS users. SSM, Super VO, VO, and IOs are required to enroll and pass the annual training, qualification, and certification testing modules via the Learning Management System which:

3.3.1.1. Provides on-demand training, ensuring consistency in SSM, Super VO, VO, and IO qualifications.

3.3.1.2. Verifies that RAPIDS users have mastered the knowledge and skills necessary to perform their jobs before accessing the system.

3.3.1.3. Provides training tailored to the needs of the RAPIDS users. **Note:** Completion of a pre-test allows users to "place" out of portions of the training previously mastered.

3.3.1.4. Allows users, once certified, to access the on-line training as a continuing job aid.

3.3.2. Completion of the DD Form 2841, *Certificate of Acceptance and Acknowledgement of Responsibilities (Registration Official)* (see **Attachment 7**) is required upon issuance of CAC to a VO/IO/LRA as part of training. All signed DD Forms 2841 shall be kept locally for training certification. **(T-1) Note:** SSM train newly assigned RAPIDS users and provide recurring training. Training ensures RAPIDS users understand their roles, security procedures, and the implications of performing these procedures correctly. Refer to the RAPIDS VO Information System web at **https://dhra.deps.mil/sites/dmdc/status/vois/SitePages.aspx** for additional training support materials.

3.4. Verifying Official/Issuing Official and Local Registration Authority. The VO/IO/LRA responsibilities are to:

3.4.1. Retrieve, limited update, transmit, and store data on the CAC eligible recipients in the DEERS database after verifying the official documentation. Some changes to an individual's database record may generate a system request to issue or revoke certificates as needed.

3.4.2. Suspend commissary, exchange, or Morale, Welfare, and Recreation privileges in DEERS, if necessary.

3.4.3. Notify the respective Service Project Office or DMDC Helpdesk when an invalid entry, lock or unlock of a record in DEERS is necessary.

3.4.4. Perform the role of the LRA as related to the PKI functions. Many of the functions are performed automatically through RAPIDS.

3.4.5. Provide and explain to the CAC recipient that their signature on the DD Form 2842, acknowledges reading and accepting their responsibilities and obligations as stated.

3.4.6. Perform CAC related processes as further described in RAPIDS User Guide.

3.5. Super Verifying Official. The Super VO also qualifies as a VO/LRA. In addition, the Super VO will be required to manage the report functions provided in D/R for the respective site and maintain the site-specific information used on the server database. (T-1)

3.5.1. Generate and examine reports at least once a week, and more often as needed, to identify performance trends, to evaluate VO accuracy, and detect possible fraudulent activities. Reports include the transaction report, identification card report, error report, and periodic summary report.

3.5.2. Delete report data on a monthly basis to free up hard drive, server, and/or shared drive space; consideration should be given to copying the data before deletion.

3.5.3. Ensure Verifying Officials read and understand the Message of the Day.

3.5.4. Train VO/LRA, Super VOs and SSM on RAPIDS using the Certification Practice Statement; RAPIDS User Guide; and the web via Verifying Officer Information System.

3.6. Site Security Manager. The SSM also qualifies as a Super VO and VO/LRA. The SSM must verify the new VO/IO/LRA is a United States citizen and has satisfied the background vetting requirement. **(T-1)** The new VO/IO/LRA should be issued a CAC if not already in possession of one with simultaneous completion of the DD Form 2841. The identity certificate is used to authenticate the new RAPIDS VO. Each site must have two SSMs and cannot operate without at least one SSM physically available to attend to all SSM duties and responsibilities. The SSMs responsibilities are collectively reflected in the Certification Practice Statement, RAPIDS User Guide, and as indicated below:

3.6.1. The SSMs are the RAPIDS user administrators for the site and are responsible for and have the authority to activate RAPIDS users and assign or change authorized roles for VO, identifications, and Super VO. Each SSM must know the RAPIDS application, rules and procedures. The DMDC Security Web User Administration tool allows each SSM to request DEERS logon identification, update security privileges for current authorized users. The SSM ensures password and PINs remain current and terminate user access of individuals no longer associated with the issuing site. Each SSM must ensure that the VO, IO, and Super VO CACs are updated with LRA privileges. Initial training of new users and subsequent training to ensure efficient and secure operations is required.

3.6.2. The SSM are responsible for the management of CAC stock and related consumables. CAC stock is ordered through a secure web-based automated card management system, known as the Inventory Logistics Portal. Refer to **Chapter 4** and the Inventory Logistics Portal User Guide for card stock and consumable order and reorder information.

3.6.3. Each SSM is responsible for management of site policies and procedures to ensure the continuous operation of the site and seamless transition of SSMs. These policies include all security policies detailed in the references stated in **paragraph 3.2**.

3.6.3.1. Each SSM must also be aware of the various procedures for maintaining a secure and productive site. **(T-1)** Key procedures are:

3.6.3.1.1. Arrange for an overlap period between the out-processing and in-processing SSM.

3.6.3.1.2. Ensure the in-processing SSM has a CAC with LRA privileges, and RAPIDS access. **Note**: SSM database access for RAPIDS can take as long as 48 hours to be effective.

3.6.3.1.3. A VO can issue a CAC to the new SSM, but only a SSM can request LRA privileges for RAPIDS users.

3.6.3.1.4. Ensure CAC issuing equipment is maintained in accordance with the RAPIDS User Guide and guidance from DMDC in accordance with the RAPIDS Security Checklist and maintain a copy on file. Refer to RAPIDS Security Standard Operating Procedure 5.1.

3.6.3.1.5. Ensure Continuity of Operations Plan and Disaster Recovery Plan are available in support of uninterrupted service. Short-term failure (3-days or less), provide customers with a list of other RAPIDS sites. Long-term failure (4-days or more), contact the Service DEERS Project Office. See **paragraph 4.4** on equipment relocation procedures.

3.6.4. Each Site Security Manager is responsible for the D/R Site Administration. DEERS is the single point of entry for vital site information and shares this information with other systems that are critical to the installation, maintenance, and support of RAPIDS. Additionally, with the Inventory Logistics Portal system, the CAC stock and supplies shall be delivered only to the site address stored in DEERS. For this reason, it is critical to maintain current site addresses, email addresses, and telephone numbers by using the DMDC Security Web function.

3.6.4.1. Changes to Site Name, Site City and State must be requested through your Service Project Office or agency office point of contact. This function includes the use of two separate addresses, one for the receipt of regular mail and another for the signature receipt of the CAC stock and supply deliveries.

3.6.4.2. Additional SSM site administration responsibilities include but are not limited to:

3.6.4.3. Complying with direction from the DMDC Support Center for viewing or updating RAPIDS Configuration Utilities.

3.6.4.4. Notifying the respective Service Project Office, DMDC Support Office or agency point of contact when an invalid entry or lock to a record in DEERS is necessary.

3.6.4.5. Maintaining an up-to-date Site Roster using the User Administration tools function.

3.6.4.5.1. Each SSM is responsible for the upkeep of current versions of related publications and articles, management of initial and continued training of site personnel, and maintenance of current RAPIDS software and server-related settings. These tasks include:

3.6.4.5.2. Ensure training of new VO/IO /LRAs, Super VOs, and SSMs on the RAPIDS web based training module, Learning Management System.

3.6.4.5.3. Training VO/IO/LRA, Super VO, and SSMs on security policies using the RAPIDS Security Standard Operating Procedure (see **Attachment 1**, Definitions).

Chapter 4

REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM SITE MANAGEMENT

4.1. Cardstock Management. SSM must use the Inventory Logistics Portal to manage the CAC stock for the issuing site.

4.1.1. The Inventory Logistics Portal is a Web-based interface operating over a secure connection and requires the identity certificate from the SSM's CAC for access.

4.1.2. The Inventory Logistics Portal will be used to replenish all CAC cardstock and related consumables. Inventory Logistics Portal automatically generates orders based on CAC cardstock levels. The reorder point is the calculated level at which an automatic replenishment order is generated via the Inventory Logistics Portal. Orders are shipped to the SSMs at the site's address location registered in DEERS.

4.1.2.1. If a CAC is printed and not encoded, the Inventory Logistics Portal will not register the card as being issued. This type of action negatively affects the Inventory Logistics Portal card stock balance.

4.1.3. When the Inventory Logistics Portal is not available or when unique circumstances warrant, order CAC cardstock using the order form from the VO Information System web site **https://dhra.deps.mil/sites/dmdc/status/vois/SitePages.aspx**.

4.1.4. Out of cycle requests for card stock must be coordinated through respective DEERS/RAPIDS Agency/Service Project Office by telephone or email.

4.2. Card Handling and Storage Guidelines. Sites are responsible for safeguarding their CAC cardstock and equipment in a secure location. **(T-3)** (Refer to the RAPIDS VO Certification Practice Statement for security procedures).

4.3. Consumables: Printer Ribbon, Laminate, Cleaning Kit. The automatic order of card stock and the consumables is done through the Inventory Logistics Portal which manages the levels of inventory at each RAPIDS site. When the Inventory Logistics Portal is not available, order CAC consumables using the order form **https://dhra.deps.mil/sites/dmdc/status/vois/SitePages.aspx**. The DMDC/Personnel Identity Protection will provide RAPIDS sites with consumables based on their CAC production volume, including color printer ribbons and laminate rolls. Additional consumable replacements are processed through the appropriate SPO to DMDC. Refer to the RAPIDS User Guide for consumable storage and destruction procedures, including equipment relocation requests.

4.4. Equipment Relocation. When relocation is required and the stated timeframes cannot be met, the SSM should submit the request by email to the Service Project Office as soon as details are known. Relocations performed without authority that result in damage or inoperable systems will result in the site providing funding for the equipment repairs and replacements and the costs associated with such. Natural disasters may create situations that will prompt actions by site personnel to secure the resources. When there is time to act and no risk to the safety of site personnel, call or email the respective Service Project Office attempting to move RAPIDS components.

4.5. Continuity of Operations Plan. "Continuity planning is simply the good business practice of ensuring the execution of essential functions through all circumstances, and it is a fundamental responsibility of public and private entities responsible to their stakeholders," Homeland Security, Federal Continuity Directive 1. All RAPIDS sites will establish a Continuity of Operations Plan/Disaster Recovery Plan in providing uninterrupted service for local customer base and quick return to operation after a system failure. **(T-3)** Reference RAPIDS Users Guide and Security Standard Operating Procedure.

Chapter 5

PERSONAL IDENTITY VERIFICATION PRIVACY REQUIREMENTS

5.1. Personal Identity Verification Requirements. Reference -12 directed a Federal standard for secure and reliable forms of ID for Federal employees and contractors, interoperable among the Federal departments and agencies. The resulting standard is Federal Information Processing Standards -201 and defines the requirements for PIV credentials issued only when an individual's identity and background have been properly vetted and positively adjudicated; strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; and support by electronic authentication.

5.1.1. The CAC is DoD PIV credential used to facilitate physical access to facilities and installations and enable logical access to DoD networks. This guidance does not address procedures or requirements related to the use of the CAC for physical access to facilities or installations or for access to DoD networks. These areas are addressed in separate DoD guidance from USD(I) and ASD(NII).

5.1.2. In addition to the current CAC capabilities, the CAC includes "contactless" technology (e.g., International Standards Organization 14443) and biometrics for personnel identification and authentication. Biometric data, such as digital fingerprints and a digital photo, are stored secured in an Integrate Circuit Chip providing capability for rapid authentication. PKI certificates stored on the card enable cardholders to "sign" documents digitally, encrypt or decrypt e-mails, and establish secure online network connections.

5.1.3. There will be population categories (including non-DoD Federal Government employees affiliated with the Department) that may still require the issuance of a CAC to support their DoD assignment, benefits entitlements, or Geneva Conventions requirements. To be issued a CAC, these individuals will be required to apply for a waiver to the CAC eligibility policy through the Office of the USD (P&R). **(T-3)** Waivers will be reviewed and granted on a case-by-case basis. **(T-3)**

5.2. Personal Identity Verification – Federal Employees And Contractors. Homeland Security Presidential Directive-12, *"Policy for a Common Identification Standard for Federal Employees and Contractors,"* August 27, 2004, establishes policy to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). Secure and reliable forms of identification for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

5.3. Early Issuance. Authoritative Data Source. CAC eligible personnel must be registered in DEERS through an authoritative personnel data feed from the appropriate Service, Agency, or the MP-ICAM, (formerly TASS). **(T-0)**

5.4. Initial Issuance – Eligibility, Affiliation, Background Vetting, And Claimed Identity. Identity Verification. During the CAC issuance process, all personnel will present two

forms of identification in original form to verify a claimed identity. **(T-0)** The identity source documents must come from the list of acceptable documents included in Form I-9, Office of Management and Budget No. 115-0136, "*Employment Eligibility Verification*." Consistent with applicable law, at least one document from the Form I-9 lists shall be a valid (unexpired) State or Federal Government-issued picture identification. **(T-0)** The identity documents will be inspected for authenticity and scanned and stored in the DEERS according to the RAPIDS User Guide upon issuance of an identification. **(T-0)** The photo identification requirement cannot be waived, consistent with applicable statutory requirements.

5.5. Replacement – Lost, Stolen, Printed Information Changed, And Card Media Damage. The CAC will be reissued when:

5.5.1. Printed information requires changes (e.g., pay grade, rank) or when any of the media (including printed data, magnetic stripe, bar codes, chip, or contactless chip) becomes illegible or inoperable. **(T-1)** The card issuer will verify the cardholder's identity against the biometric information stored in DEERS. **(T-3)** Consistent with applicable law, the applicant shall be required to provide identity source documents. **(T-3)**

5.5.2. The CAC is reported lost or stolen. The card issuer will verify the cardholder's identity against the biometric information stored in DEERS and confirm the expiration date of the missing CAC. **(T-3).** The individual shall be required to present documentation from the local security office or CAC sponsor confirming that the CAC has been reported lost or stolen. **(T-3)** This documentation must be scanned and stored in RAPIDS. **(T-3)** The individual reporting a lost, stolen, or destroyed ID shall be required to provide identity source documents as noted on **Attachments 4**, **Attachment 10**, and **Attachment 11**. **(T-3)** The replacement CAC will have the same expiration date as the lost or stolen card. **(T-3)**

5.6. Expiration Dates. Local commands, installations, and sponsors of contract support personnel and other eligible CAC Card holders will establish procedures to ensure that the issuance and retrieval of CAC are part of the normal personnel check-in and check-out processes. **(T-3)** These procedures will identify who will have responsibility to retrieve CAC from government personnel leaving government service and for any sponsored contract support personnel who are no longer supporting their organization and/or activity. **(T-2)** These CAC will be documented and treated as personally identifiable information or identification of a person, according to DoDI 5400.11 and DoDM 5200.01, Vol 3, *DoD Information Security Program: Protection of Classified Information,* and returned to a RAPIDS site for disposition. **(T-2)**

5.6.1. Invalid, inaccurate, inoperative, terminated, or expired CAC shall be returned to a RAPIDS site for disposition. The CAC is the property of the US Government and shall not be retained by the cardholder upon expiration, replacement, or when the DoD affiliation of the employee has been terminated. **Note:** CAC is issued with a three-year expiration date. **Exception**: Services academies - CAC are issue with a 4-year expiration date with a three-year PKI certificate.

5.7. Common Access Card Public Key Infrastructure Certificates. Using RAPIDS, the identity certificate will be issued on the CAC at the time of card issuance in compliance with the X.509 *Certificate Policy for the United States Department of Defense.* **(T-2)** E-mail signature and e-mail encryption certificates may also be available on the CAC either upon issuance or at a later time, including the availability of the PIV Authentication. If the person receiving a CAC does not have an organization e-mail address assigned to them, they may return to a RAPIDS terminal, user

maintenance portal, or post issuance portal to receive their e-mail certificate when the e-mail address has been assigned. Upon loss, destruction, or revocation of the CAC, the certificates thereon are revoked and placed on the certificate revocation list according to X.509 *Certificate Policy for the United States Department of Defense.* All other situations that pertain to the disposition of the certificates are handled according to X.509 *Certificate Policy for the United States Department of Defense* as implemented.

5.8. Multiple Common Access Card Issuance. There are individuals within DoD who have multiple DEERS Personnel Category Codes with the Department (e.g., an individual that is both a reservist and a contractor). They shall be issued a separate identification card in each personnel category for which they are eligible. **(T-1)** Multiple current identification cards will not be issued or exist for an individual under a single Personnel Category Code in DEERS. **(T-0)**

5.9. Limited Off-line Issuance of Temporary Common Access Card. If a member has been mobilized and there are no communications either with DEERS or the CA, a temporary card can be issued with an abbreviated expiration date for a maximum of 10 days. The temporary card will not have Public Key certificates and will be replaced as soon as the member can reach an online RAPIDS station or communications have been restored. **(T-2)**

5.10. Photograph Requirements. The photo identification requirement cannot be waived, consistent with applicable statutory and uniformed Services and Agencies requirements. Photographs will consist of frontal pose, full-face without head apparel (except as stated in **paragraph 5.10.1**) or body piercing accoutrements, etc. **(T-0)** The following provides general guidance concerning photographs for the CAC:

5.10.1. Individual will pose with a frontal, full-face (passport-type) photo shot. **(T-3)** Individual's composure will reflect similar to guidelines posted by the US Department of State for passport issuance listed at **www.travel.state.gov/passport**. **(T-3)** Head covering is acceptable for medical and religious reasons provided that the face is in full view. Photo cut-off is below shoulders when in military clothing, so insignia, badges, and emblems are not visible.

5.10.2. Military personnel may be photographed while wearing uniform or civilian clothes.

5.10.3. Active, Selected Reserves, National Guard, and Participating Individual Ready Reserve (PIRR) members must comply with their respective Service grooming standards. **(T-1) Note:** Active, Selected Reserve, PIRR, and Volunteer Training Unit members must also be within Service dress and appearance standards when in civilian attire. **(T-1)** This also applies to members who are on appellate leave. Refer to DAFI 36-3026, Volume 1, paragraph 9.4.

5.10.4. Nonparticipating individual Reserve members, Standby, and Retired Reserve (awaiting pay at age 60) do not have comply with their respective Service dress and grooming standards, when issued the DD Form 2 (Reserve). Refer to DAFI 36-3026, Volume 1.

5.10.5. Photographs will have no title board or sign visible, clothing is visible and have no discernible words, effects, or designs voiding a person's identity or affecting the legibility of the card information. **(T-1)**

5.10.6. Photographs must have a plain background without unit designations, motifs, or flag displays; white is recommended, light shades of neutrals may be used in lieu of white. **Note:**

Anything other than the authorized background will render the card invalid and require reissuance of the card.

Chapter 6

RAPIDS ASSISTANCE POINTS OF CONTACTS

6.1. Uniformed Services DEERS/RAPIDS Project Offices.

6.1.1. *ACTIVE/RESERVE/RETIRED ARMY* - DEPARTMENT OF THE ARMY, US Army Human Resources Command, 1600 Spearhead Division Avenue, Fort Knox, KY 40122, (502) 613-8461 / 9029 or 1-888-276-9472, Fax (502) 613-9535, E-mail: **usarmy.knox.hrc.mbx.tagd-deers@mail.mil**.

6.1.2. *ARMY GUARD* - National Guard Bureau, ARNG-HRP-P (Personnel Actions Branch), 111 South George Mason Drive, Arlington, Virginia 22204-1382, 1-866-810-9183, (703) 607-9751 or Defense Switch Network 327-9751. Fax: (703) 607-8448 or Defense Switch Network: 327-8448.

6.1.3. *ACTIVE/RETIRED NAVY* - DEPARTMENT OF THE NAVY, My Navy Career Center, 5720 Integrity Drive, Millington, Tennessee 38055-6730, (833) 330-6622.

6.1.4. *NAVY RESERVE* - Commander Naval Reserve Forces, Attn: 221, 4400 Dauphine Street, New Orleans, Louisiana 70146-5000, (504) 678-3959/4259 or Defense Switch Network 678-3959/4259. Fax: (504) 678-6137.

6.1.5. *ACTIVE/RETIRED AIR FORCE AND SPACE FORCE* - DEPARTMENT OF THE AIR FORCE, AFPC/DP3SA, 550 C Street West, JBSA Randolph Texas 78150-4739, Total Force Service Center (TFSC) for all inquiries,1-800-525-0102. Tier 2 case management, (210) 565-2089.

6.1.6. *AIR FORCE RESERVE/AIR NATIONAL GUARD* - HQ AIR RESERVE PERSONNEL CENTER, 18420 East Silver Creek Ave Bldg 390, MS68, Buckley SFB, Colorado 80011, (720) 847-3886 or Defense Switch Network 847-3886; Fax (720) 847-3886, Defense Switch Network 847; E-mail: **tfsc_2@mypersmail.af.mil**.

6.1.7. *AIR FORCE TOTAL FORCE SERVICE CENTER (San Antonio)* - Active, ANG, Reserve, Retired, Civilian, Contractor Personnel, and DEERS Beneficiaries 1-800-525-0102; Civilian employee Common Access Card research / resolution requests to **afpoa.a1.sd@us.af.mil**.

6.1.8. *ACTIVE MARINE CORPS* - Headquarters, US Marine Corps, Manpower, and Reserve Affairs (MFP-1), 2008 Elliot Road, Quantico, Virginia 22134-5103, (703) 784-9529 or Defense Switch Network 278-9529.

6.1.9. *MARINE CORPS RESERVE* - Commander, MARFORRES (G-1), RM 4E7604, 2000 Opelousas Ave, New Orleans Louisiana 70114-1500, (504) 697-7180/7273 or Defense Switch Network 647-7180/7272. Fax: (504) 697-9773.

6.1.10. *RETIRED MARINE CORPS* - Headquarters, US Marine Corps, Manpower and Reserve Affairs (MMSR-6), 2008 Elliot Road, Quantico, Virginia 22134-5103: (703) 784-9188 or Defense Switch Network 278-9188. Retirees and their eligible family members, or survivors may call (800) 336-4649. Fax (703) 784-9834.

6.1.11. *ACTIVE/RESERVE COAST GUARD* - UNITED STATES COAST GUARD, US Coast Guard, Personnel Service Center (PSC), US Coast Guard Stop 7200, 2703 Martin Luther King, Jr., Ave SE, Washington, DC 20593-7200, (202) 795-6642.

6.1.12. *RETIRED COAST GUARD* – Commanding Officer (RAS), US Coast Guard Pay and Personnel Center, 444 SE Quincy Street, Topeka, KS 66683-3591, 1-800-772-8724, (785) 339-3441. Fax (785) 339-3770.

6.1.13. *ACTIVE/RETIRED* NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION - Commissioned Personnel Center CPC1, 8403 Colesville Road, Suite 500, Silver Spring, Maryland 20910-3282, (301) 713-0850, ext. 158. Fax: (301) 713-4140.

6.1.14. *ACTIVE/RESERVE RETIRED UNITED STATES PUBLIC HEALTH SERVICE* - UNITED STATES PUBLIC HEALTH SERVICE, Commissioned Corps Headquarters, 1101 Wootton Parkway, Suite 300, Rockville, Maryland 20852, (240) 453-6000. Fax: (240) 453-6134, E-mail: **phsdeersgibill@hhs.gov**.

6.1.15. *FEDERAL AGENCIES CVS or* Trusted Associate Sponsorship System Enrollments - (202) 776-8906.

6.2. DEFENSE MANPOWER DATA CENTER SUPPORT HELPDESK: continental United States. Ft Knox, KY, 1-800-3-RAPIDS (1-800-372-7437), Defense Switch Network 878-2856 (country code 312).

6.2.1. DMDC SUPPORT OFFICE (DSO). 400 Gigling Road, Seaside, California 93955-6771, (831) 583-2500 or Defense Switch Network: 878-3261/2659 or 3335. Fax (831) 655-8317 or (831) 644-9256.

6.2.2. Point of contact for health care eligibility questions: United States 1-800-538-9552, TTY /TDD 1-866-363-2883, Germany 0800-1013161, Italy 800-783784, United Kingdom 08-005871594, Korea 00798-14-800-5570, Philippines 1-800-1-114-1235, and Japan 00531-1-20731.

6.3. DEFENSE MANPOWER DATA CENTER SUPPORT HELPDESK - DMDC SUPPORT CENTER-Asia (DSC-A). Yongsan Army Garrison, Bldg S5450, Seoul South Korea 140-766; telephone 82-2-7916-6198 (DSC-Asia main number), 82-2-7916-6197, Defense Switch Network 315-736-6198/6197, E-mail: **helpdesk-dsoa@korea.army.mil**.

6.4. DEFENSE MANPOWER DATA CENTER SUPPORT CENTER-Europe (DSC-E): US Hospital/AM Kirchberg, 1st Street, Geb 3701, 2-OG, 66849 Landstuhl, Deutschland. Army Post Office Address: HQ LRMC, CMR402 ATTN: DSC-E, Defense Switch Network: 486-7365, Commercial: +49(0)6371-86-7365; Fax: +49(0)6371-86-7672.

6.5. Social Security Administration. For Social Security enrollment and eligibility information: 1-800-772-1213. SSA Web site: **www.ssa.gov**. Medicare Web site: **www.medicare.gov**.

BRIAN L. SCARLETT, SES, DAF
Principal Deputy Assistant Secretary of the
Air Force for Manpower and Reserve Affairs

KEVIN M. KENNEDY, USN
Commander, Navy Personnel Command
JAMES F. GLYNN, Lt General, USMC

Deputy Commandant for
Manpower and Reserve Affairs
STEVEN E. DAY, RADM, USCG

Acting Director of Reserve and Military Personnel
CHAD M. CARY, RADM
Director, National Oceanic and Atmospheric
Administration Corps

RICHARD P. SCHOBITZ, RDML, USPHS
Director, Commissioned Corps Headquarters

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5, United States Code, Section 2105(a) "*Employee*" Sections 311, 2102, 2103, 2105, 3132, and 5311-5318 of Title 5, United States Code

Title 18, United States Code, Sections 499, 506, 509, 701, and 1001, *Crimes and Criminal Procedure*

Title 10, United States Code, Chapter 1209, *Selected Reserve*

Deputy Secretary of Defense Memorandum, *Policy Guidance for Provision of Medical Care to Department of Defense Civilian Employees Injured or Wounded While Forward Deployed in Support of Hostilities,* 24 September 2007

Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* 27 August 2004

Office of Management and Budget Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – *Policy for a Common Identification Standard for Federal Employees and Contractors,* 5 August 2005

Federal Information Processing Standards Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS 201-3), January 2022

Under Secretary of Defense for Personnel and Readiness Memorandum, *DEERS/RAPIDS Lock Down for Contractors,* 10 November 2005

Assistant Secretary of Defense for Health Affairs Memorandum, *Medical Care Costs for Civilian Employees Deployed in Support of Contingency Operations,* 8 January 1997

DoD 1400.25-M, *DoD Civilian Personnel Manual,* 1 December 1996

DoDI 1000.01, *Identity Cards Required by the Geneva Convention,* 16 April 2012

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

DoDI 1000.25, *DoD Personnel Identity Protection (PIP) Program,* 2 March 2016

DoDI 1330.09, *Armed Services Exchange Policy*, 7 December 2005

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

DoDI 3020.41, *Operational Contract Support (OCS),* 20 December 2011

DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, 10 December 2005

DoDI 5400.11, *DoD Privacy and Civil Liberties Programs,* 29 January 2019

DoDI 8500.01, *Cybersecurity,* 14 March 2014

DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK)* Enabling, 18 May 2023

DoDI 8910.01, *Information Collection and Reporting,* 5 December 2022

DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* 23 January 2014

DoDM 1000.13, Volume 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,* 23 January 2014

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information,* February 24, 2012, Incorporating Change 2, 1 October 2020

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

Directive-type Memorandum (DTM) 17-004, *Department of Defense Expeditionary Civilian Workforce,* 23 January 2024

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

DAFMAN 90-161, *Publishing Processes and Procedures*, 17 October 2023

DAFI 36-3026, Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel,* 31 May 2023

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

Defense Manpower Data Center (DMDC), *DoD Implementation Guide for CAC Next Generation Version 2.6,* November 2006

DMDC, *DoD Implementation Guide for CAC PIV End-Point version 1.0,* 17 December 2007

Defense Manpower Data Center, *Trusted Associate Sponsorship System, formerly Contractor Verification System (CVS) User Guide,* August 2013

Office of Management and Budget (OMB) M-05-24, *Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors,* 5 August 2005

OPM Memorandum, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12,* 31 July 2008

Office of Personnel and Management (OPM) Federal Investigations Notice 06-04, *HSPD-12 – Advanced Fingerprints Results,* 8 June 2006

Real-time Automated Personnel Identification System 7.1 *User Guide*, May 2016

Section 701 of Title 18, United States Code X.509 *Certificate Policy for the United States Department of Defense,* 9 February 2005

Adopted Forms

DD Form 577, *Appointment/Termination Record – Authorized Signature*

DAF Form 847, *Recommendation for Change of Product*

DD Form 1172-2, *Application for Department of Defense Common Access Card DEERS Enrollment* (formerly *DD Form 1172, Application for Uniformed Services Identification Card-DEERS Enrollment*

DA Form 1602, *Civilian Identification Card (Accountable)*

DD Form 2841, *Department of Defense (DoD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities*

DD Form 2842, *Subscriber Certificate Acceptance and Acknowledgement of Responsibilities*

USCIS Form I-9, *Employment Eligibility Verification" and Lists of Acceptable Documents*

Abbreviations and Acronyms

ADP—Automated Data Processing Level II

AFRC—Air Force Reserve Command

AHRC—Army Human Resources Command-Fort Knox

CA—Certificate Authority

C&A—Certification and Accreditation

CO—contracting officer

COR—Contracting Officer Representative

CP—X.509 Certificate Policy

CtO—Certificate to Operate

DEERS—Defense Enrollment Eligibility Reporting System

IP—Internet Protocol

IO—Issuing Official

LRA—Local Registration Authority

MP ICAM—Mission Partner Identity, Credentialing and Access Management

NATO—North Atlantic Treaty Organization

NOAA—National Oceanic and Atmospheric Administration

PKI—Public Key Infrastructure

PIP—Personnel Identity Protection

PIV—Personal Identity Verification

RA—Registration Authority

RAPIDS—Real Time Automated Personnel Identification System

SPO—Service Project Office

SSA—Social Security Administration

TASS—Trusted Associate Sponsorship System

VO—Verifying Official

UMP/PIP—User Maintenance Portal/Post Issuance Portal

USCG—United States Coast Guard

USPHS—United States Public Health Service

Terms

Access to a Department of Defense Network—User logon to a Windows active directory account on the NIPRNet or an authorized network operating system account on the NIPRNet.

Access to a Department of Defense Network (Remote)—Authorized NIPRNet users accessing a NIPRNet resource from: Another NIPRNet resource outside of the originating domain; or an authorized system that resides outside of the NIPRNet. This includes domain-level access from handheld devices. Remote access includes logon for the purposes of telework, Virtual Private Network, and remote administration by DoD or non-DoD personnel, (including USCG, NOAA, and USPHS).

Authorizing/Verifying Official for DD Form 1172-2—The authorizing official may be in the position of COR, Quality Assurance Evaluator, Contracting Officer Technical Representative, the designated CO assigned to the installation contracting office, or the installation's designated representative. The individual shall be a member of the Uniformed Services or a Federal/Government/DoD employee. When individual is not a RAPIDS VO/LRA, the Authorizing/VO shall be designated by a completed DD Form 577, Signature Card or signature memorandum one of which must be on file at the issuing facility.

Background Investigations—An investigation required for determining the eligibility of an applicant for PIV credentialing.

Certificate of Networthiness—Issued by the Services' communications communities validating the Systems Security Authorization Agreement for a specified period of time. The system change is processed through a series of tests; the tests are documented and based on the results; a determination is made as to whether there are risks. Mitigations are recommended and implemented or, justification is provided explaining why the systems change request is not implemented. The Designated Approval Authority determines the risk and approves or disapproves the system change request.

Certificate to Operate (CtO)—Issued by Service commands permitting local networks to accept the application for which certified.

Certificate Policy X.509 (CP)—Defines DoD PKI policy and outlines Service requirements.

Certification and Accreditation (C&A)—Certification of an IT system is a comprehensive evaluation of the technical and non-technical security feature of that system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design implementation meets a set of specified security requirements. Accreditation of an IT system is a formal declaration by the Designated Approval Authority that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. The process established by the DoD for Certification and Accreditation of unclassified and classified IT systems is called the DITSCAP.

Certification Authority (CA)—An authority trusted by one or more users to create and assign certificates.

Certification Practice Statement—Describes how VOs/LRAs meet the requirements set forth in the CP policy.

Certificate Management Authority—Certification Authority (CA) or Registration Authority (RA).

Certificate-related Information—Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.

Certificate Status Authority—A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.

Chipless Card—Temporary card used in lieu of the CAC.

Civilian Employee—DoD civilian employees (both appropriated and non-appropriated), as defined in section 2105 of title 5, United States Code are individuals appointed to positions by designated officials (including USCG, NOAA, and USPHS). Appointments to appropriated fund positions are either permanent or time-limited and the employees are on full-time, part-time, or intermittent work schedules. In some instances, the appointments are seasonal with either a full-time, part-time, or intermittent work schedule. Positions are categorized further as Senior Executive Service, Competitive Service, and Excepted Service positions. In addition, the DoD employs individuals paid from non-appropriated funds, as well as foreign national citizens outside the United States, its territories, and its possessions, in DoD activities overseas. The terms and conditions of host-nation citizen employment are governed by controlling treaties, agreements, and memorandums of understanding with the foreign nations.

Common Access Card—Contains 4 certificates: Identity, E-mail Signing, E-mail Encryption, and PIV Authentication. The PIV certificate enables the CAC to be Homeland Security Presidential Directive-12 compliant and interoperable with other Federal Agencies and their PKI. Since August 24, 2014, the CAC is issued with the PIV certificate activated.

Competitive Service Positions—Appointments to appropriated fund positions based on selection from competitive examination registers of eligibles or under a direct hire authority. See section 2102 of Sections 311, 2102, 2103, 2105, 3132, and 5311-5318 of title 5, United States Code.

Contingency—A military operation that (a) is designated by the Secretary of Defense as an operation in which members of the Armed Forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force; or (b) results in the call or order to, or retention on, active duty of members of the uniformed services under section 688, 12301(a), 12302, 12304, 12305, or 12406 of title 10, chapter 15, or any other provision of law during a war or during a national emergency declared by the President or Congress. See contingency operation. See JP 1-02.

Contingency Contractor Personnel—Defense contractors and employees of defense contractors and associated subcontractors as defined in Reference (x), including US citizens, US legal aliens, third country national personnel, and citizens of host nations, who are authorized to accompany US military forces in contingency operations, other military operations, or exercises designated by the geographic combatant commander (including USCG, NOAA, and USPHS). This includes employees of external support, systems support, and theater support contractors.

Contractor Employee—An employee of a firm, or individual under contract or subcontract to the DoD, designated as providing services or support to the Department who requires physical and/or logical access to the facilities and/or systems of the Department (including USCG, NOAA, and

USPHS). For the purposes of CAC issuance and expiration dates on the CAC, an individual is considered under contract for the base plus any option periods, regardless of contract funding status (i.e., an individual under a multi-year contract with only the base year funded can be issued a CAC that expires in a maximum of 3 years so long as the CAC can be revoked upon termination of the contract).

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 such as the RAPIDS and other programs within DoD and the military departments.

Dependent—An individual whose relationship to the sponsor leads to entitlement to benefits and privileges; pertains to of legal marriage and family members only. See Family Member Term in DAFI 36-3026, Volume 1.

Defense Agencies and Offices—All agencies and offices of the DoD, including Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Contract Management Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency/Central Security Service.

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)—The standard DoD approach for identifying information security requirements, providing security solutions, and managing information system security activities.

Deployable and Shipboard (Portable REAL TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM)—This platform integrates RAPIDS workstation and server functionality eliminating the need for a separate server**.**

Designated Approval Authority—The authority that signs the Systems Security Authorization Agreement and Certification and Accreditation letter certifying the system is safe for implementation. The Designated Approval Authority accepts full responsibility should the system be later determined to be unsafe.

Excepted Service Positions—All appropriated fund positions in the Department that specifically are excepted from the competitive service by or pursuant to statute, by the President, or by Office of Personnel Management, and which are not in the Senior Executive Service. Individuals also may be appointed to the competitive service by conversion from another appointment, such as a Veterans Rehabilitation Act appointment. Excepted service appointments include student career program appointments and student temporary employment program appointments. See section 2103 of Sections 311, 2102, 2103, 2105, 3132, and 5311-5318 of title 5, United States Code.

Federally Controlled Facility—Includes the following: Federally owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of a department or agency; Federally controlled commercial space shared with non-Government tenants. (for example, if a department or agency leased the 10th floor of a commercial building, the guidance in this DAFI applies to the 10th floor only); Government-owned, contractor-operated facilities, including laboratories

engaged in national defense research and production activities; and Facilities under a management and operating contract, such as for the operation, maintenance, or support of a Government-owned or -controlled research, development, special production, or testing establishment.

Federally Controlled Information System—An information system used or operated by a Federal agency, or a contractor or other organization on behalf of the agency.

Federal Information Processing Standards (FIPS-201)—The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act of 2002. This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.

Foreign National Civilians and Contractors—A category of personnel that, for the purpose of this guidance, are CAC eligible if sponsored by their government as part of an official visit or assigned to work on a DoD facility and/or require access to DoD networks both on site or remotely (remote access must be on an exception only basis for this category). Personnel in this category are not paid by the United States and are not entitled to any benefits administered by the Department.

Foreign National Positions (Direct Hire)—See section 1581 of Title 10, United States Code Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, as amended.

Foreign National Positions (Indirect Hire)—See section 1581 of Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, as amended.

Foreign Affiliate Personnel—The card will reflect the Equivalent (EQ) rank, example “Major.” The DoD/uniformed Service sponsoring agency should validate the rank equivalent and include it on official documentation, i.e., the DD-Form 1172-2, memorandum, or travel order at card issuance, replacement, or update. Here are the personnel: Sponsored NATO and Partnership For Peace personnel in the United States**.** Active duty officer and enlisted personnel of NATO and Partnership For Peace countries serving in the United States under the sponsorship or invitation of the DoD or a Military Department. Sponsored non-NATO personnel in the United States. Active duty officer and enlisted personnel of non-NATO countries serving in the United States under the sponsorship or invitation of the DoD or a Military Department. NATO and non-NATO personnel outside the United States **-** AD officer and enlisted personnel of NATO and non-NATO countries when serving outside the United States and outside their own country under the sponsorship or invitation of the DoD or a Military Department, or when it is determined by the major overseas commander that the granting of such privileges is in the best interests of the United States and such personnel are connected with, or their activities are related to the performance of, functions of the US military establishment. Non-sponsored NATO personnel in the United States. AD officer and enlisted personnel of NATO countries who, in connection with their official NATO duties, are stationed in the United States and are not under the sponsorship of the DoD or a Military Department, are not eligible for a CAC, and will continue to receive a DD Form 2765.

Full-time Work Schedule—Full-time employment with a basic 40-hour workweek.

Grades Authorized for Common Access Card Issuing/Verifying/Local Registration Authorization Officials—Commissioned officers, Warrant Officer, Enlisted personnel, Civilian employee General Schedule, contractor employee. **Note:** The senior personnel official may appoint in writing, other responsible military personnel, federal civilian and contractor personnel, regardless of rank or pay grade to verify and issue an identity credential such as a CAC or Volunteer Logical Access Credential if the mission requires it. See DAFI 36-3026, Volume 1, Issuing/Verifying Official Term.

Government Sponsor—Based on the DoD government sponsor's determination (including USCG, NOAA, and Public Health Service) of the type, and frequency of access required to DoD facilities, or networks that will effectively support the mission.

Homeland Security Presidential Directive-12—A Federal Standard for secure and reliable forms of ID. Use of ID by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.

Identification Card Office Online (IDCO) —IDCO replaced Real-time Automated Personnel Identification System Self-Service (RSS) portal which replaced the User Maintenance Portal (UMP)/Post Issuance Portal (PIP) functionality used for adding or updating E-mail addresses and to receive initial or new Public Key E-mail signature and E-mail encryption certificates, add a Personal Category Code to the User Principle Name of E-mail encryption certificates, add a Personnel Category Code to the User Principle Name of E-mail certificate, activation of the PIV certificate, and adding the Joint Data Model applet to the CAC.

Identity Proofing—The process providing sufficient pre-determined evidence (Form I-9 documents) to tie the individual authoritatively to the identity established within the identity management system. This data collection is undertaken during the identity vetting process.

Identity Vetting—Activity associated with building up sufficient credible, referenced documentation and associated data to provide reasonable evidence of personal identity; the collection and aggregation of sufficient positively referenced data to establish the attributes of identity within the identity management systems; and processing and validating personal identity against law enforcement and terrorist databases.

Inactive National Guard—The Inactive National Guard is part of the Army National Guard. These individuals are Reservists who are attached to a specific National Guard unit, but who do not participate in training activities. On mobilization, they shall mobilize with their assigned units. These members muster with their units once a year.

Individual Ready Reserve—Trained individuals who have previously served in the active component or Selected Reserve and have time remaining on their Military Service Obligation. It also includes volunteers, who do not have time remaining on the Military Service Obligation but are under contractual agreement to be a member of the Individual Ready Reserve. These individuals are mobilization assets and may be called to AD under the provisions of Chapter 1209 of 10 United States Code (reference [u]). Also includes untrained individuals.

Information system—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Integrated Circuit Chip—A small piece of semiconducting material (usually silicon) on which an integrated circuit is embedded. A typical chip can contain millions of electronic components (transistors).

Intergovernmental Personnel Act Employees—The Intergovernmental Personnel Act mobility program provides temporary assignment of personnel between the Federal government and State and local governments, colleges and universities, Indian tribal governments, Federally funded research and development centers, and other eligible organizations.

Intermittent Work Schedule—Employment without a regularly scheduled tour of duty.

Local Hire Appointment—An appointment that is made from among individuals residing in the overseas area. For example, the appointment could be a career conditional appointment or an excepted appointment with termination of the appointment triggered by the sponsor's rotation date.

Local Registration Authority—An individual trained to act as the trusted agent/entity to validate the identity of a customer seeking electronic (eAuthentication) to the network. The role of the Local Registration Authority can be compared to the registration process of "identity proofing."

Member—An individual who is affiliated with a Service, either AD, Reserve, or Guard, or an Agency, either a civilian or contractor (also includes other eligible personnel for DEERS enrollment).

Mission Partner Affiliation Sponsor (MPAS)—MPAS replaced the former Trusted Agent (TA) role with the TASS, formerly the Contractor Verification System (CVS). MP-ICAM replaced the TASS TA Security Manager or TA. MPAS and Mission Partner Affiliation Security Manager (MPASM) must be certified, trained, and US citizen and a US government employee, US military or US DoD civilian, and possess a valid CAC. The MP-ICAM MPAS/MPASM duties are separate, by ensuring the enrollment authority (via MP-ICAM web application) and the issuance authority (via RAPIDS workstation) are not the same entity (shared duties), in accordance with Federal Identity Processing Standard 201.

National Agency Check with Written Inquiries—A personnel security investigation combining a National Agency Check and written inquires to law enforcement agencies, former employers and supervisors, references, and schools. All National Agency Check with Inquiries conducted for DoD shall include a credit check.

Non-appropriated Funds Employees—. Federal employees within the DoD who are paid from non-appropriated fund.

NIPRNET—Non-Secure Internet Protocol Router Network is used to exchange sensitive but unclassified information between users as well as providing users' access to the Internet.

Permanent Appointment—Career or career conditional appointment in the competitive or Senior Executive Service and an appointment in the excepted service that carry no restrictions or conditions.

Participating Individual Ready Reserve—Consists of those Ready Reservists who are not in the Selected Reserve and are in a non-pay training program. Members in this category (e.g., USAF Academy Liaison Officers) are attached to an active or reserve component unit.

Part-time Work Schedule—Part-time employment of 16 to 32 hours a week under a schedule consisting of an equal or varied number of hours per day.

Permanent Appointment—Career or career conditional appointment in the Senior Executive Service, Competitive Service, or an appointment in the Excepted Service that carries no restrictions or conditions.

Public Key Infrastructure—Framework established to issue, maintain, and revoke public key certificates.

Public Key Infrastructure Sponsor—Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects and is responsible for meeting the obligations of Subscribers as defined throughout the X.509 Certificate Policy for the United States DoD.

Personal Identity Verification—February 25, 2005, the National Institute of Standards and Technology released Federal Information Processing Standards - 201 in response to Homeland Security Presidential Directive-12, Common Identification Standard for Federal employees and contractors. Federal Information Processing Standards-201, PIV of Federal Employees and Contractors, includes the architecture and technical requirements for a government-wide PIV system in which common identification credentials can be issued and verified. The underlying objective of Federal Information Processing Standards - 201 is to provide a secure and efficient method for verifying identity of individuals seeking physical access to Federally controlled government facilities and logical access to government information systems.

Personal Identity Verification Card—The PIV card is the primary component of the PIV system and is used to authenticate with various physical and logical resources. To meet the security and interoperability objectives set forth in Homeland Security Presidential Directive-12, PIV cards must use consistent technology and have a common look with consistent placement of printed components. For a complete look at the mandatory and optional physical components of a PIV card, refer to section 4.1 of Federal Information Processing Standards-201.

Real-time Automated Personnel Identification System—A network of microcomputers linking the Uniformed Services Personnel Offices to the DEERS database to provide on-line processing of information to the DEERS database.

Ready Reserve—Military members of the National Guard and Reserve, organized in units or as individuals, liable for recall to active duty to augment the active components in time of war or national emergency. The Ready Reserve consists of three Reserve component subcategories: the Selected Reserve, the IRR, and the Inactive National Guard.

Registration Authority (RA)—Entity responsible for identification and authentication of certificate subjects that have automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.

Seasonal Employment—Annually recurring periods of work of less than 12 months each year. Seasonal employees generally are permanent employees who are placed in non-duty and/or non-

pay status and recalled to duty according to pre-established conditions of employment. Seasonal employees may have full-time, part-time, or intermittent work schedules.

Servicing Security Office—The security office assigned responsibility for providing security support to the organization responsible for CAC applicants.

Senior Executive Service Positions—DoD non-appropriated fund employees in positions at the NF-6 pay-band level, including appropriated fund positions in an agency classified above General Schedule-15 pursuant to section 5108 or in level IV or V, or an equivalent position, which is not required to be filled by an appointment by the President by and with the advice and consent of the Senate and for which an employee performs the functions listed in section 2105.

Sponsor—A member on active duty or civil servant who approves a CAC request.

Unterminated Common Access Card—A valid CAC with at least a valid identity certificate.

Verifying Official (VO)/Local Registration Authority (LRA)—A person who is a U.S. citizen and authorized by the Chief of Issuing Activity or per job description to perform the role of a VO/LRA as a military member, DoD contractor or civilian (appropriated or non-appropriated fund—supported), equivalent civilian personnel employed by the National Guard of the United States, responsible for issuing identification cards. For VO this also includes other similarly qualified personnel in exceptional cases as determined by the Secretary of the Military Department, or a designee, responsible for validating eligibility of bona fide beneficiaries to receive benefits and entitlements.

Signature Certificate—A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

SIPRNet—is a system of interconnected computer networks to transmit classified/secret information by Transmission Control Protocol IP.

Smart Card—A credit card-size device, normally for carrying and use by personnel, that contains one or more integrated circuits and may also employ one or more of the following technologies: magnetic stripe; bar codes, linear or two dimensional; non-contact and radio frequency transmitters; biometric information; encryption and authentication; photo identification.

Security Policy Compliance Assessment (SPCA)—Consists of a review of the Systems Security Authorization Agreement for security policy issues.

Social Security Number Documentation—Any government document showing social security number: e.g., original Social Security Card, passport, driver's license, W-2 Form, Standard Form 50, Leave and Earning Statement.

Special Agent—For purposes of this instruction, a special agent is defined as an agent of the US Army Criminal Investigations Command; Naval Criminal Investigative Service; Air Force Office of Special Investigations; Marine Corps, Naval Criminal Investigative Service; and USCG Intelligence.

Special Agent Offices—US Army Criminal Investigative Command; Naval Criminal Investigative Service; Air Force Office of Special Investigations; Marine Corps, Naval Criminal Investigative Service; and USCG Intelligence.

Subscriber—An entity that 1) is the subject named or identified in a certificate issued to such an entity, and 2) holds a private key that corresponds to a public key listed in that certificate 3) Investigation Requirement.

Temporary Appointment—An appointment for a specified period not to exceed 1 year. A temporary appointment can be extended up to a maximum of 1 additional year.

Term Appointment—An appointment for a period of more than 1 year but not more than 4 years to a position where the need for an employee's services is not permanent. In the Excepted Service, the proper designation for an equivalent appointment is time-limited with an appropriate not-to-exceed date.

Verifying Official/Local Registration Authority Certification Process—VO/LRA must be certified, trained, and a US citizen. They will be routinely audited to ensure the duties and responsibilities set forth in the CP and the Certification Practice Statement are being properly performed to include verifying that a CAC recipient has appropriate identification; completing and correctly disposing of the forms involved in the CAC issuance process and collecting and disposing of any CAC or other identification cards returned.

Voluntary Training Unit—A unit formed by volunteers to provide Reserve Component training in a non-pay status for IRR and active status Standby Reservists attached under competent orders and participating in such units for retirement points. Also, called reinforcement training unit or mobile training unit.

Attachment 2

COMMON ACCESS CARD ENTITLEMENT TABLES

A2.1. Refer to DoDM 1000.13, Volume 2, regarding CAC Table Entitlement.

Attachment 3

BASIC DOCUMENTATION OR ACCEPTABLE INFORMATION SOURCES FOR SPONSORHIP IN DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM

A3.1. Basic Documentation. Basic documentation or acceptable information sources for sponsorship in DEERS. In all cases refer to **Table A3.1** and **Table A3.2**. **Note:** Under Secretary of Defense, Personnel and Readiness (USD [P&R]) Memorandum, October 29, 2010, *"DEERS/RAPIDS Lock Down for Contractors,"* November 2005, DoD identification card eligible populations shall have their information entered and verified in DEERS using a secure automated personnel data feed by the MP-ICAM, (formerly TASS), or as determined by the DMDC and the sponsoring Service/Agency. **(T-1)** Non-US person non-appropriated fund employees shall continue to have their information manually entered at a RAPIDS workstation via DD Form 1172-2. **(T-1)**

Table A3.1. Required Documentation For Determining Sponsorship.

Personnel Status	Documentation/Information Source/Sponsorship
Civilian Affiliate	Civil Service (Other Federal Agency) – verified DD Form 1172-2. Enrolled in MP-ICAM and approval for CAC issuance from the MPAS. **Note:** DHRA/DMDC approval is required for other federal agency employees (non-DoD civil service). Includes non-federal agency associates – verified DD Form 1172-2. Refer to the appropriate uniformed Services MP-ICAM Service Point of Contact (SPOC) regarding use of DD Form 1172-2.
Contractor	Contractor (DoD and Uniformed Service) – enrolled in MP-ICAM and approved for CAC issuance. **Note:** DHRA/DMDC approval is required for other federal agency employees (non-DoD civil service). Includes non-federal agency associates – verified DD Form 1172-2Refer to the appropriate uniformed Services MP-ICAM SPOC regarding use of DD Form 1172-2.
DoD Civilian Employee	Civil Service (DoD and Uniformed Service) – Defense Civilian Personnel Data System (DCPDS) enrollment to DEERS. DoD Overseas Continental United States Local Hire – verified DD Form 1172-2. Non-appropriated funds Employee (DoD and Uniformed Services) – verified DD Form 1172-2. **Note:** Refer to the appropriate uniformed Services MP-ICAM SPOC regarding use of DD Form 1172-2.
Foreign Affiliate	Foreign military AD member – Invitational travel order or other document reflecting sponsorship by the DoD or uniformed Service or verified DD Form 1172-2. Requires MP-ICAM enrollment and

	MPAS approval for CAC issuance. **Note:** The card will reflect the Equivalent (EQ) rank, example "Major." The DoD/uniformed Service sponsoring agency will validate the rank equivalent and include it on official documentation, i.e., the DD-Form 1172-2, memorandum, or Invitational travel order at card issuance, replacement, or update. Foreign national civilian – verified DD Form 1172-2. Requires MP-ICAM enrollment and MPAS approval for CAC issuance. **Note:** Refer to the appropriate uniformed Services MP-ICAM SPOC regarding use of DD Form 1172-2.
Presidential Appointee	Presidential Appointee – verified by Defense Manpower Center/PIP Solutions Division.
Uniformed Services Member	Academy – Service Academy Cadets, Midshipmen, Coast Guard Cadets and Merchant Marine Academy Midshipmen – Cadet or Midshipman's Personnel Office or Director of Science Merchant Marine Academy at Kings Point, NY, as appropriate. Active duty – DEERS, Personnel Data System, a current document from the personnel record, i.e., DD Form 4, Extended Active Duty Order, etc., or an order that specifies 31 days or more. National Guard and Reserve members of the Selected Reserve – DEERS, Personnel Data System, a current document in the personnel record, i.e., Commissioning Oath, DD Form 4, DD Form 214, Separation Orders.

A3.1.1. There are four CAC types used within the DoD/Uniformed Services, based on eligibility. Refer to DoD website **www.cac.mil** for each CAC description.

Table A3.2. Documentation Required To Determine Type Of Common Access Card For Civilian And Contractor Employees.

Personnel Status	Common Access Card	Documentation/Information source
Civilian employees	Identification CAC	Defense Civilian Personnel Data System enrollment to DEERS, or
	Identification and Privilege CAC (For overseas assignment, card is issued in Overseas Continental United States)	Verified DD Form 1172-2 as supported by 1. SF Form 50 and/or DD Form 1614, Request and Authorization for DoD Civilian Permanent Duty Travel assigning the employee for more than 365 days Overseas Continental United States. Transportation Agreement. 2. Document requiring employee to reside on military installation in Continental United States Hawaii or Alaska.

	Geneva Conventions CAC for Civilians Accompanying the Armed Forces	1. DD Form 2365, Overseas Emergency Essential Position Agreement. 2. DD Form 1610, Request for Authorization for Temporary Duty Travel of DoD Personnel or other official document directing travel as a civilian noncombatant to a region of conflict, combat or contingency operations who may be liable to capture and detention as a Prisoner of War.
Contractor Employees	Identification CAC	MP-ICAM, (formerly TASS) enrollment to DEERS.
	Identification and Privilege CAC (For overseas assignment, card is issued in Overseas Continental United States)	Verified DD Form 1172-2 as supported by: 1. Synchronized Pre-deployment Operational Tracker/Letter of Authorization document. 2. Statement of Work or contract that stipulates duration of Overseas Continental United States assignment for more than 365 days. Transportation Agreement. 3. Document requiring contractor employee to reside on military installation in Continental United States, Hawaii or Alaska. 4. Letter of Identification or other official document directing travel
	Geneva Conventions CAC for Civilians Accompanying the Armed Forces	Verified DD Form 1172-2 as supported by 1. Synchronized Pre-deployment Operational Tracker/Letter of Authorization document. 2. Statement of Work designating contractor employee as a contingency/essential contractor. If their Statement of Work doesn't support their designation as essential/contingency, they would only qualify for the ID CAC and would use their orders. 3. Letter of Identification or other official document directing travel as a civilian noncombatant to a region of conflict, combat or contingency operations who may be liable to capture and detention as a Prisoner of War.

A3.1.2. CAC eligible individuals requiring enrollment to DEERS through a personnel data feed contact the respective Service DEERS/RAPIDS/PKI Project Office, Department Agency, or the DMDC Support Office. See **Chapter 6**, UNIFORMED SERVICES DEERS/RAPIDS PROJECT OFFICES, DMDC SUPPORT CENTER (DSC).

Attachment 4

DEPARTMENT OF DEFENSE LIST OF ACCEPTABLE IDENTITY DOCUMENTS

A4.1. See DoD List of Acceptable Identity Documents for identity proofing, DEERS enrollment, eligibility, and ID card issuance purposes at: https://www.cac.mil/Portals/53/List_of_Acceptable_Documents.pdf?ver=2019-08-20-130159-397.

Attachment 5

INSTRUCTIONS FOR COMPLETION OF DD FORM 1172-2, "APPLICATION FOR IDENTIFICATION CARD/DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM ENROLLMENT"

A5.1. DD Form 1172-2. Instructions.

A5.1.1. The DD Form 1172-2 shall be used to apply for issuance of a USID and a CAC for eligible individuals who are not enrolled in the DEERS or to update eligible individual's DEERS record. **(T-0)** Refer to DoDM 1000.12, Volume 1, for background vetting requirements to qualify for issuance of the CAC. Retention and disposition of the DD Form 1172-2 shall be in accordance with uniformed services' regulatory instructions. **(T-0)**

A5.1.2. DoD sponsors enrolling their dependents in DEERS should complete Sections I, II, and IV.

A5.1.3. DoD sponsors updating their own status or adding a personnel condition impacting benefits (e.g., overseas assignment) should complete Sections I and II.

A5.1.4. Eligible employees applying for a CAC should complete Sections I and II (and Section IV if a Foreign Affiliate on orders to the US with authorized Dependents). The DD Form 1172-2 should then be provided to a DoD Sponsor for authorization and completion of Section III.

A5.1.5. DoD sponsors authorizing a CAC for an employee should complete Section III.

A5.1.6. For certain populations a paper form will not be required. **(T-2) Note:** Applicable populations are those entered into RAPIDS via MP-ICAM (formerly TASS).

A5.1.7. A DD Form 577 (Signature card) must be on file at the issuing site for CAC applicants using the DD Form 1172-2 for enrollment. **(T-2)**

A5.2. SECTION I. SPONSOR/EMPLOYEE INFORMATION.

A5.2.1. Block 1. Name. Enter the sponsor/employee's LAST name first, enter the FIRST name, and then enter the MIDDLE INITIAL or the full MIDDLE NAME. (Use no more than 51 characters.) The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial. The name cannot contain any special characters nor is any punctuation permitted.

A5.2.2. Block 2. Sex. Enter the sponsor/employee's sex from the valid codes listed in **Table A5.1**: (Use one character code M or F that represents the applicant's biological sex.

Table A5.1. DD Form 1172-2 Block. Sex Abbreviations.

Code	Sex
M	Male
F	Female

A5.2.3. Block 3. Social Security Number or DoD ID Number.

A5.2.4. Enter the sponsor/employees' Social Security Number or DoD ID Number. In cases where an employee has not been issued an Social Security Number or DoD ID Number, an

ITIN can be provided. If neither number is available, a Foreign Identification Number will be generated by the system. A Foreign Identification Number (assigned as 900-00-0000F and up) will be assigned and automatically generated for eligible foreign affiliate and foreign nationals who do not have an Social Security Number. An Social Security Number or ITIN is the preferred identifier for initial enrollment. Only in cases where neither is available should an alternate be used.

A5.2.5. For VOs: If a Social Security Number or DoD ID Number is already registered in DEERS for another individual, STOP processing and verify the number. If verification confirms duplication of the Social Security Number by the Social Security Administration, continue processing and the system shall automatically generate a duplicate control number for the additional sponsor. **(T-1)**

A5.2.6. Block 4. Status. Enter the sponsor/employee status from the valid codes listed in **Table A5.2**. If unsure of status, leave blank. (Use no more than six characters.)

Table A5.2. DD Form 1172-2 Block 4 Status.

CODE	STATUS
ACADMY	Academy or Navy Officer Candidate School Student
AD	Active duty (excluding Guard and Reserve on extended active duty for more than 30 days)
AD-DEC	Active duty deceased
CIV	Civilian
CONTR	Contractor
DAVDEC	100-percent disabled veteran deceased (either temporary [TMP] or permanent [PRM])
DAVPRM	100-percent disabled veteran, permanent disability
DAVTMP	100-percent disabled veteran, temporary disability
FP	Foreign affiliate personnel
FMRMR	Former member who is in receipt of retired pay for non-regular service but who has been discharged from the Service and maintains no military affiliation
FMRDEC	A former member who qualified for retired pay for non-regular service at his or her sixtieth birthday, before his or her discharge from the Service, but died while in receipt of retired pay
GRD	National Guard (all categories)
GRDDEC	National Guard deceased
GRD-AD	Guard on extended active duty for more than 30 days
MH	Medal of Honor recipient
MH-DEC	Medal of Honor recipient deceased
OTHER	Non-DoD eligible beneficiaries (including credit union employees, and other civilians employed in support of US forces overseas, who are authorized benefits and privileges)
PDRL	Retired member, on the Permanent Disability Retired List
PR-APL	Prisoner or Appellate leave
RCL-AD	Recalled to active duty

RES	Reserve (all categories)
RES-AD	National Guard and Reserve members who retire, but are not entitled to retired pay until age 60
RESDEC	Reserve deceased
RESRET	National Guard and Reserve members who retire, but are not entitled to retired pay until age 60
RET	Retired member entitled to retired pay
RETDEC	Deceased retired member entitled to retired pay. Code applies to active duty retired, Retired Reserve beginning on their 60th birthday, the temporary disability retired list, and the permanent disability retired list.
SSB	Special Separation Benefits recipient member with 120 days medical benefits (CHAMPUS/TRICARE and Medical Treatment Facility)
TDRL	Retired member, on the temporary disability retired list
TA-RES	Selected Reserve Transition Assistance Management Program members and their eligible dependents
TA-30	Involuntarily separated member of Reserve or Guard Component entitled to 30 days medical benefits (CHAMPUS/TRICARE and Medical Treatment Facility)
TA-60	Involuntarily separated member with 60 days medical benefits (CHAMPUS/TRICARE and Medical Treatment Facility)
TA-120	Involuntarily separated member with 120 days medical benefits (CHAMPUS/TRICARE and Medical Treatment Facility)
TA-180	Involuntarily separated member with 180 days medical benefits (CHAMPUS/TRICARE and Medical Treatment Facility). **Exceptions:** See DAFI 36-3026, Volume 1, Chapter 6 for sole survivorship discharge or separating from AD and agree to become a member of the Selected Reserve of the Ready Reserve of a Reserve Component.
VSI	Voluntary Separation Incentive recipient with 120 days medical benefits (CHAMPUS/TRICARE and Medical Treatment Facility)

A5.2.7. Block 5. Organization. Enter the sponsor/employee's organization or branch or service from the valid codes listed in **Table A5.3** (Use no more than five characters.)

Table A5.3. DD Form 1172-2 Block 5 Organization.

CODE	ORGANIZATION
USA	US Army
USAF	US Air Force
USN	US Navy
USMC	US Marine Corps
USCG	US Coast Guard
USPHS	US Public Health Service
NOAA	National Oceanic and Atmospheric Administration
DoD	Department of Defense
FED	Employee of an Agency other than DoD

OTHER	Used when the sponsor is not affiliated with one of the uniformed services listed above

A5.2.8. Block 6. Pay Grade. Enter the sponsor/employee pay grade from the valid codes listed in **Table A5.4** (Use no more than four characters.)

Table A5.4. DD Form 1172-2 Block 6 Pay Grade.

CODE	BRANCH OF SERVICE
EI-E9	Enlisted pay grades 1 through 9
W1-W5	Warrant officers pay grades 1 through 5
STDT	Academy and/or Navy Officer Candidate School student (ENTER PAY GRADE IF STDT RECEIVING PAY)
001-011	Officer pay grades 1 through 11 (011 is reserved)
GS-01 – GS-18	Federal employees with General Schedule pay grades
NF1-NF6	Federal employees with Nonappropriated Fund pay grades
OTHER	Other (non-uniformed service) pay grades not defined above to include all contractors
N/A	Not applicable. Use this code with the Block 4 status codes of "FMRMR" or FMRDEC"

A5.2.9. Block 7. GEN CAT (Geneva Convention Category). Leave this block blank. This block is automatically generated by D/R with the valid codes listed in **Table A5.5**.

Table A5.5. DD Form 1172-2 Block 7. Geneva Category.

CODE	GEN CAT
I	Category I (pay grades E1 through E4)
II	Category II (pay grades E5 through E9)
III	Category III (pay grades W1 through 003 and/or Cadets and/or Midshipmen)
IV	Category IV (pay grades 004 through 006)
V	Category V (pay grades 007 through 011)
N/A	Not applicable (non-protected personnel)

A5.2.10. Block 8. Citizenship. Enter the sponsor/employee's appropriate country of citizenship from the valid codes listed in **Table A5.6** (Use two characters.)

Table A5.6. DD Form 1172-2 Block 8 Country Abbreviations.

COUNTRY	CODE	COUNTRY	CODE	COUNTRY	CODE
Afghanistan	**AF**	**Germany**	**GM**	**Nigeria**	**NI**

Albania	AL	Ghana	GH	Niue	NE
Algeria	AG	Gibraltar	GI	Norfolk Island	NF
America Samoa	AQ	Glorioiso Islands	GO	Northern Mariana Islands	CQ
Andorra	AN	Greece	GR	Norway	NO
Angola	AO	Greenland	GL	Oman	MU
Anguilla	AV	Grenada	GJ	Pakistan	PK
Antarctica	AY	Guadeloupe	GP	Palmyra Atoll	LQ
Antigua and Barbuda	AC	Guam	GQ	Panama	PM
Argentina	AR	Guatemala	GT	Papua New Guinea	PP
Armenia	AM	Guernsey	GK	Paracel Islands	PF
Aruba	AA	Guinea	GV	Paraguay	PA
Ashmore and Cartier Islands	AT	Guinea-Bissau	PU	Peru	PE
Australia	AS	Guyana	GY	Philippines	RP
Austria	AU	Haiti	HA	Pitcairn Islands	PC
Azerbaijan	AJ	Heard Island and McDonald Islands	HM	Poland	PL
Bahamas, The	BF	Honduras	HO	Portugal	PO
Bahrain	BA	Hong Kong	HK	Puerto Rico	RQ
Baker Island	FQ	Howland Island	HQ	Qatar	QA
Bangladesh	BG	Hungary	HU	Reunion	RE
Barbados	BB	Iceland	IC	Romania	RO
Bassas Da India	BS	India	IN	Russia	RS
Belarus	BO	Indonesia	ID	Rwanda	RW
Belgium	BE	Iran	IR	St. Kitts and Nevis	SC
Belize	BH	Iraq	IZ	St. Helena	SH
Benin	BN	Ireland	EI	St. Lucia	ST
Bermuda	BD	Israel	IS	St. Pierre and Miquelon	SB
Bhutan	BT	Italy	IT	St. Vincent and the Grenadines	VC
Bolivia	BL	Ivory Coast	IV	San Marino	SM
Bosnia and Herzegovina	BO	Jamaica	JM	Sao Tome and Principe	TP
Botswana	BC	Jan Mayen	JN	Saudi Arabia	SA
Bouvet Island	BV	Japan	JA	Senegal	SG
Brazil	BR	Jarvis Island	DQ	Serbia	SR
British Indian Ocean Territory	IO	Jersey	JE	Seychelles	SE

British Virgin Islands	VI	Johnston Atoll	JQ	Sierra Leone	SL
Brunei	BX	Jordan	JO	Singapore	SN
Bulgaria	BU	Juan De Nova Island	JU	Slovakia	LO
Burkina	UV	Kazakhstan	KZ	Slovenia	SI
Burma	BM	Kenya	KE	Solomon Islands	BP
Burundi	BY	Kingman Reef	KQ	Somalia	SO
Cambodia	CB	Kiribati	KR	South Africa	SF
Cameroon	CM	Korea, Democratic	KN	South Georgia and the South Sandwich Islands	SX
Canada	CA	Korea, Republic of	KS	Spain	SP
Cape Verde	CV	Kuwait	KU	Spratly Islands	PG
Cayman Islands	CJ	Kyrgyzstan	KG	Sri Lanka	CE
Central African Republic	CT	Laos	LA	Sudan	SU
Chad	CD	Latvia	LG	Surinam	NS
Chile	CI	Lebanon	LE	Svalbard	SV
China	CH	Lesotho	LT	Swaziland	WZ
Christmas Island	KT	Liberia	LI	Sweden	SW
Clipperton Islands	IP	Libya	LY	Switzerland	SZ
Cocos (Keeling) Islands	CK	Liechtenstein	LS	Syria	SY
Colombia	CO	Lithuania	LH	Taiwan	TW
Comoros	CN	Luxembourg	LU	Tajikstan	TI
Cook Islands	CW	Macau	MC	Tanzania	TZ
Coral Sea Islands	CR	Macedonia	MK	Thailand	TH
Costa Rica	CS	Madagascar	MA	Togo	TO
Cote Dtvoire	IV	Malawi	MI	Tokelau	TL
Croatia	HR	Malaysia	MY	Tonga	TN
Cuba	CU	Maldives	MV	Trinidad and Tobago	TD
Cyprus	CY	Mali	ML	Tromelin Island	TE
Czech Republic	EZ	Malta	MT	Trust Territory of the Pacific Islands (Palau)	PS
Denmark	DA	Man, Isle of	IM	Tunisia	TS
Djibouti	DJ	Marshall Islands	RM	Turkey	TU

Dominica	DO	Martinique	MB	Turkmenistan	TX
Dominican Republic	DR	Mauritania	MR	Turks and Caicos Islands	TK
Ecuador	EC	Mauritius	MP	Tuvalu	TV
Egypt	EG	Mayotte	MF	Uganda	UG
El Salvador	ES	Mexico	MX	Ukraine	UP
Equatorial Guinea	EK	Midway Islands	MQ	United Arab Emirates	TC
Eritrea	ER	Moldova	MD	United Kingdom	UK
Estonia	EN	Monaco	MN	United States	US
Ethiopia	ET	Mongolia	MG	Uruguay	UY
Europa Island	EU	Montenegro	MW	Uzbekistan	UZ
Falkland Islands (Islas Malvinas)	FK	Montserrat	MH	Vanuatu	NH
Faroe Islands	FO	Morocco	MO	Vatican City	VT
Federated States of Micronesia	FM	Mozambique	MZ	Venezuela	VE
Fiji	FJ	Namibia	WA	Vietnam	VM
Finland	FI	Nauru	NR	Virgin Islands	VQ
France	FR	Navassa Island	BQ	Wake Island	WQ
French Guiana	FG	Nepal	NP	Wallis and Futuna	WF
French Polynesia	FP	Netherlands	NL	West Bank	WE
French Southern and Antarctic Lands	FS	Netherlands Antilles	NA	Western Sahara	WI
Gabon	GB	New Caledonia	NC	Western Samoa	WS
Gambia, The	GA	New Zealand	NZ	Yemen (Aden)	YM
Gaza Strip	GZ	Nicaragua	NU	Zambia	ZA
Georgia	GG	Niger	NG	Zimbabwe	ZI

A5.2.11. Block 9. Date of Birth. Enter the sponsor/employee's date of birth four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD). (Use nine characters.)

A5.2.12. Block 10. Place of Birth. Enter the sponsor/employee's place of birth, including (City, State, and Country, if outside the United States). Enter the State abbreviations of the sponsor/employee's place of birth from the valid codes provided in **Table A5.7**. If place of birth is a foreign country, enter the country from the valid codes from **Table A5.6**.

Table A5.7. DD Form 1172-2 Block 10 Place of Birth.

STATE	CODE	STATE	CODE	STATE	CODE

Europe & Canada	**AE**	**Kansas**	**KS**	**Oklahoma**	**OK**
Alabama	**AL**	**Kentucky**	**KY**	**Oregon**	**OR**
Pacific	**AP**	**Louisiana**	**LA**	**Pennsylvania**	**PA**
Alaska	**AK**	**Maine**	**ME**	**Puerto Rico**	**PR**
American Samoa	**AS**	**Maryland**	**MD**	**Rhode Island**	**RI**
Arizona	**AZ**	**Massachusetts**	**MA**	**South and Central America**	**AA**
Arkansas	**AR**	**Michigan**	**MI**	**South Carolina**	**SC**
California	**CA**	**Minnesota**	**MN**	**South Dakota**	**SD**
Colorado	**CO**	**Mississippi**	**MS**	**Tennessee**	**TN**
Connecticut	**CT**	**Missouri**	**MO**	**Federated States of Marshall Islands, Palau**	**TT**
Delaware	**DE**	**Montana**	**MT**	**Texas**	**TX**
District of Columbia	**DC**	**Nebraska**	**NE**	**Utah**	**UT**
Florida	**FL**	**Nevada**	**NV**	**Vermont**	**VT**
Georgia	**GA**	**New Hampshire**	**NH**	**Virginia**	**VA**
Guam	**GU**	**New Jersey**	**NJ**	**Virgin Islands**	**VI**
Hawaii	**HI**	**New Mexico**	**NM**	**Washington**	**WA**
Idaho	**ID**	**New York**	**NY**	**West Virginia**	**WV**
Illinois	**IL**	**North Carolina**	**NC**	**Wisconsin**	**WI**
Indiana	**IN**	**North Dakota**	**ND**	**Wyoming**	**WY**
Iowa	**IA**	**Ohio**	**OH**		

A5.2.13. Block 11. Current Home Address. Enter the number and street of the sponsor/employee's current residence address. If sponsor is deceased or if address is unknown, leave blank. (Use no more than 27 characters.)

A5.2.14. Block 12. City. Enter the sponsor/employee's current city of residence. If the sponsor's address is an Army Post Office or a Fleet Post Office, enter the designation Army Post Office or Fleet Post Office. If the sponsor is deceased or city is unknown, leave blank. (Use no more than 18 characters.)

A5.2.15. Block 13. State. Enter the correct US postal code for the State of the sponsor/employee's residence from the valid codes listed in **Table A5.7** (Use two characters.) If the sponsor/employee's address is an Army Post Office or Fleet Post Office, enter the correct Army Post Office or Fleet Post Office State. If the sponsor/employee lives outside of the 50 United States, the District of Columbia, or one of the listed trust territories, enter a default value of "XX." (Use two characters.) If the sponsor is deceased or if State is unknown, leave blank.

A5.2.16. Block 14. Zone Improvement Plan Code. Enter the correct nine-digit Zone Improvement Plan Code of the sponsor's current residence address in the following format: "123456789." If the last four digits are unknown, enter four zeros (0000); e.g., "123450000." If the sponsor does not reside in one of the 50 United States, the District of Columbia, or one of the listed trust territories, enter the applicable foreign Zone Improvement Plan Code, or Army Post Office or Fleet Post Office number. If the sponsor is deceased or if Zone Improvement Plan Code is unknown, leave blank. (Use no more than nine characters.)

A5.2.17. Block 15. Country. Enter the employee's correct country of residence from the valid abbreviations listed in **Table A5.6**. If the sponsor/employee's address is an Army Post Office or Fleet Post Office, the country must be "US" (use two characters.) If country is unknown, leave blank.

A5.2.18. Block 16. Primary e-mail address. Enter the sponsor/employee's office/work e-mail address as applicable. This block may be left blank.

A5.2.19. Block 17. Telephone Number. Enter the sponsor/employee's current residence, duty, or business telephone number beginning with the area code. Do not use punctuation to separate area code, prefix, and basic number. This block may be left blank. (Use no more than 10 characters.)

A5.2.20. Block 18. City of Duty Location. Enter the city of the sponsor/employee's duty location.

A5.2.21. Block 19. State of Duty Location. Enter the correct US postal code for the State of the sponsor/employee's duty location from the valid codes listed in **Table A5.7**. If the sponsor's address is an Army Post Office or Fleet Post Office, enter the correct Army Post Office or Fleet Post Office State. If the sponsor lives outside of the 50 United States, the District of Columbia, or one of the listed trust territories, enter a default value of "XX." (Use two characters.) If the sponsor is deceased or if State is unknown, leave blank.

A5.2.22. Block 20. Country of Duty Location. Enter the correct Country of the sponsor/employee's duty location from the valid codes listed in **Table A5.6** (Use two characters.) If the country is not listed, leave blank.

A5.3. SECTION II – SPONSOR/EMPLOYEE DECLARATION AND REMARKS.

A5.3.1. Block 21. Remarks. Enter the method of verification and further explanation of qualifying status, such as SF 52, sponsoring agency, and period of DEERS enrollment, or indicate other appropriate comments, such as particular work assignment. This section may be left blank, or prepopulated by the VO. **Note:** DD Form 1172-2: *Application for Identification Card/DEERS Enrollment,* the former DD 1172 signature block in Section V has been removed. VOs must include their name, RAPIDS site ID, telephone, & signature in block 21. If a VO did not generate the DD Form 1172-2, sponsor must sign & notarize in Section II before accepted at any identification card issuing facility.

A5.3.2. Block 22. Sponsor /Employee Signature. Block must contain the sponsor/employee's signature, with the following exceptions:

A5.3.2.1. Unremarried or Unmarried former spouses shall sign for themselves. **(T-3)**

A5.3.2.2. When the sponsor is deceased each of the survivors (widow, widower, children, parent, parent in-law, and stepparent) shall sign for themselves. **(T-3) Note:** When the

surviving spouse is a stepparent, do not have the stepparent sign authorizing the surviving child of the sponsor to receive an identification card. Each person's information within the record is protected by the Privacy Act Statement.

A5.3.2.3. When the sponsor is unavailable for signature, the VO shall ensure that the dependency between the sponsor and family member exists. **(T-1)** See **paragraph A5.3.2.4** and **paragraph A5.3.2.5** below.

A5.3.2.4. A valid general or special power of attorney is acceptable if the sponsor is unavailable to sign. VO will annotate on block 21 the power of attorney presented by the beneficiary. **(T-1)**

A5.3.2.5. When the sponsor is unable to sign the DD Form 1172-2 in the presence of the VO at the time of DEERS enrollment, the signature must be notarized. **(T-1)** The notary seal and signature should be placed in the right margin of Section II, Block 21.

A5.3.2.6. Block 23. Date Signed. Enter the date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) that block 22 was signed on the DD Form 1172-2.

A5.4. SECTION III – AUTHORIZED BY (DoD Common Access Card Sponsors Only).

A5.4.1. Block 24. Sponsoring Office Name. Enter the name of the organization the employee works for or is assigned to.

A5.4.2. Block 25. Contract Number. Enter the contract number for the purposes of entry into the MP-ICAM, (formerly TASS).

A5.4.3. Block 26. Sponsoring Office Address. Enter the number and street, city, state, Zone Improvement Plan code, and country code (see **Table A5.6** for country codes and **Table A5.7** for state abbreviations) of the employee's sponsoring office address.

A5.4.4. Block 27. Sponsoring Office Telephone Number. Enter the sponsoring office telephone number beginning with the area code. Do not use punctuation to separate area code, prefix, and basic number. (Use no more than 14 characters.)

A5.4.5. Block 28. Office Email Address. Enter the sponsor/employee's office e-mail address as applicable.

A5.4.6. Block 29. Overseas Assignment. Enter the sponsor/employee's country of assignment from the valid list of abbreviations in **Table A5.6**.

A5.4.7. Block 30. Overseas Assignment Begin Date. Enter the appropriate employee's effective begin date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) for their overseas assignment. Obtain this information from the employee's personnel documents, e.g., Travel Authorization.

A5.4.8. Block 31. Overseas Assignment End Date. Enter the employee's effective end date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) of their overseas assignment. The period of employment may be obtained from the employee's Travel Authorization.

A5.4.9. Block 32. Eligibility Effective Date. Enter the date in four digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) the employee's qualifying status began.

A5.4.10. Block 33. Eligibility Expiration Date. Enter the employee effective end date, not to exceed three years. Use four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD).

A5.4.11. Block 34. Sponsoring Official Name. Enter the name of the sponsoring official. (Use no more than 51 characters.)

A5.4.12. Block 35. Unit/Organization Name. Enter the unit and/or command name for the sponsoring official. (Use no more than 26 characters.)

A5.4.13. Block 36. Title. Enter the sponsoring official's title. (Use no more than 24 characters.)

A5.4.14. Block 37. Pay Grade. Enter the pay grade of the sponsoring official (Use no more than four characters.)

A5.4.15. Block 38. Signature. The sponsoring official must sign in that block. **(T-0)** The DoD sponsoring official shall be a uniformed service member, or civilian employee working for the sponsoring organization. **(T-0)**

A5.4.16. Block 39. Date Verified. Enter the date in four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) that block 38 was signed on the DD Form 1172-2.

A5.5. SECTION IV – VERIFIED BY.

A5.5.1. Block 40. VO Name (Last, First, Middle Initial). Enter the VO's LAST name first, enter the FIRST name, and then enter the MIDDLE initial or the full MIDDLE name. Use no more than 51 characters.

A5.5.2. Block 41. Site ID. Enter the VO's 6-digit site identification.

A5.5.3. Block 42. Telephone Number (Include Area Code/Defense Switch Network). Enter the VO's current residence, duty, or business telephone number beginning with the area code. Use no more than 10 characters. Do not use punctuation to separate area code, prefix, and basic number.

A5.5.4. Block 43. Signature. VO must sign in the block. **(T-0)**

A5.6. SECTION V – DEPENDENT INFORMATION.

A5.6.1. Block 44. Name. Enter the dependent's LAST name first, enter the FIRST name, and then enter the MIDDLE INITIAL or the full MIDDLE NAME. (Use no more than 51 characters.) The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial. The name cannot contain any special characters nor is any punctuation permitted.

A5.6.2. Sex. Enter the dependent's sex from the valid codes listed in **Table A5.1** (Use one character code; M or F, which represents the dependent's biological sex.

A5.6.3. Block 46. Date of Birth. Enter the dependent's date of birth in four-digit year, three alpha character month, and two-digit day format (YYYYMMMDD).

A5.6.4. Block 47. Relationship. Enter the dependent's relationship to the sponsor from the valid abbreviations listed in **Table A5.8**.

Table A5.8. DD Form 1172-2 Block 45 Relationship Codes.

CODE	RELATIONSHIP STATUS
CH	Child
DB	DoD Beneficiary
FC	Foster Child
PAR	Parent
PL	Parent-in-law
PACH	Pre-adoptive Child
SP	Spouse
SC	Stepchild
STP	Stepparent
SPL	Stepparent-in-law
UMW	Unmarried Widow(er)
URW	Unremarried Widow(er)
WARD	Ward
Former Spouse	DoD Beneficiary

A5.6.5. Block 48. Social Security Number or DoD Identification Number. Enter the dependent's Social Security Number, DoD identification number, ITIN or Temporary Identification Number (TIN). A TIN will automatically be generated by RAPIDS and assigned for categories of beneficiaries who do not yet have Social Security Numbers, such as newborns and foreign spouses, awaiting a Social Security Number, or for those who do not have and are not eligible for a Social Security Number. Direct care at a Medical Treatment Facility will be suspended if a Social Security Number is not provided within 270 days. **(T-1)** For initial enrollment a Social Security Number, ITIN or TIN is preferred, and an alternate should not be used unless the Social Security Number, ITIN or TIN is unavailable.

A5.6.6. Block 49. Current Home Address. Enter the number and street of the dependent's current residence address.

A5.6.7. Block 50. Primary E-mail Address. Enter the dependent's preferred e-mail address as applicable. This block may be left blank. For dependents aged 18 and older, check "Permission to use for benefits notifications (18 and above)" to verify permission for DoD to contact the included email address with DoD and Department of Veterans Affairs related benefits notifications.

A5.6.8. Block 51. Telephone Number. Enter in dependent's primary telephone number beginning with the area code. Use no more than 10 characters. Do not use punctuation to separate area code, prefix, and basic number. This block may be left blank.

A5.6.9. Block 52. City. Enter the dependent's current city of residence. If the dependent's address is an Army Post Office or Fleet Post Office, enter the designation Army Post Office or Fleet Post Office.

A5.6.10. Block 53. State. Enter the correct US postal code for the State of the dependent's residence from the valid codes listed in for block 10. (Use two characters.)

A5.6.11. Block 54. Zone Improvement Plan Code. Enter the correct nine-digit Zone Improvement Plan Code of the dependent's current residence address in the following format: "123456789." If the last four digits are unknown, enter four zeros (0000); e.g., "123450000." If the dependent does not reside in one of the 50 United States, the District of Columbia, or one of the listed trust territories, enter the applicable foreign Zone Improvement Plan Code, or Army Post Office or Fleet Post Office number.

A5.6.12. Block 55. Country. Enter the dependent's correct country of residence from the valid abbreviations listed in the instructions for Block 8. If the dependent's address is an Army Post Office or Fleet Post Office, the country must be "US." (Use two characters.) **(T-0)** If country is unknown, leave blank.

A5.6.13. Block 56. Eligibility Effective Date. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), when the dependent's qualifying status began.

A5.6.14. Block 57. Eligibility Expiration Date. Leave blank.

A5.6.15. Blocks 58-71, Enter information following the instructions in Section A.

A5.7. SECTION VI – RECEIPT.

A5.7.1. Signature. ID card recipient must sign in that block. **(T-0)** If the recipient is incapable of signing, the condition must be indicated in that block. **(T-0)**

A5.7.2. Block 73. Date Issued. Enter the date in four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), the recipient's acknowledgment of receiving an ID card. Use nine characters.

A5.8. DD FORM 1172-2, *APPLICATION FOR IDENTIFICATION CARD/DEERS ENROLLMENT*, APR 2012: template can be found at **https://www.cac.mil/Resources/**

Attachment 6

SAMPLE SIGNATURE AUTHORIZATION LETTER AND DD FORM 577, "APPOINTMENT/TERMINATON RECORD – AUTHORIZED SIGNATURE"

MEMORANDUM FOR Uniformed Services Identification (ID) Card Facility (date)

FROM: (Name of Agency, Department, or Office)

SUBJECT: Signature Authorization Letter for DD Form 1172-2 Verification

This is to certify the following individual(s) is/are appointed as a Verifying Official for Signature Authorization concerning the DD Form 1172-2, Application for the Identification Card - DEERS Enrollment:

(First, Middle, Last Name) (Signature)

Point of contact is (First, Middle, and Last Name), telephone (area code, country code, commercial/Defense Switched Network) or email (address).

//Signed//
Commander/Agency

Delegated Representative

Notes:
1. A Common Access Card recipient cannot verify him or herself on the Signature Authorization Letter or on the DD Form 577.
2. Refer to **https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0577.pdf** for DD Form 577 and instructions.

Attachment 7

DD FORM 2841, "DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES"

A7.1. The DD Form 2841 is digitally produced by the RAPIDS workstation and the subscriber (CAC recipient who is a LRA/VO) digitally signs the form by entering their PIN.

Attachment 8

DD FORM 2842, DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES (SUBSCRIBER)

A8.1. The DD Form 2842 is digitally produced by the RAPIDS workstation and the subscriber (CAC recipient) digitally signs the form by entering their PINs.

Attachment 9

RETURNING COMMON ACCESS CARD TO DEFENSE MANPOWER DATA CENTER SUPPORT CENTER

A9.1. Mail Instructions: Mail all returned or found CAC via FedEx, to the DMDC (address below). Cards are to be mailed after a thirty-day period for most sites and after collection of 20 CAC for low-volume sites. Do not cut, mutilate, or blacken the Integrate Circuit Chip with a marker for recovered CAC as testing on defective cards must be performed.

A9.2. Returning Common Access Cards by FedEx.

A9.2.1. All CAC must be returned by FedEx using the DEERS/RAPIDS account number so your site will not incur associated shipping costs. **(T-3) Note:** This account is monitored and should not be used to forward the DoD 1172-2 form or for any maintenance actions. All other uses are prohibited. For questions, contact the DMDC Support Center at 1-800-3RAPIDS or 1-800-372-7473.

A9.2.2. Follow the steps below to complete a CAC mail back:

A9.2.2.1. Complete Section 1, including a commercial phone number.

A9.2.2.2. Complete Section 3:

Defense Manpower Data Center Support Center (DMDC)
2102 E. 21st Street N.
Wichita, KS 67214

A9.2.2.3. Under Section 4a, mark block 20, the FedEx Express Saver checkbox.

A9.2.2.4. Under Section 7, Payment, mark the Third Party checkbox and Use the following

A9.2.2.5. FedEx Account Number: 2283-7326-5

A9.2.2.6. Fill out a coversheet including the number of CACs being returned and your site's contact information.

A9.2.2.7. Place returned CACs, individual CAC Return Forms for each CAC, and Coversheet into a FedEx envelope or package.

A9.2.2.8. Affix the FedEx Air bill to the package and arrange for pickup or drop off.

A9.2.2.9. Remove and retain the back copy of the FedEx Air bill (labeled Recipient's Copy) for your records IAW the Air Force Records Disposition Schedule.

Attachment 10

REAL TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM (RAPIDS) SITE SECURITY MANAGER (SSM)/VERIFYING OFFICIAL(VO)/ ISSUING OFFICIAL (IO) PROCEDURES FOR LOST, STOLEN, OR DESTROYED IDENTIFY CREDENTIAL – COMMON ACCESS CARD

A10.1. Real Time Automated Personnel Identification System Site Security Manager/VO/IO Procedures For Lost, Stolen, or Destroyed Identity Credential – Common Access Card. According to DoDM 1000.13-M-V1, paragraph 5 c (3), …" The individual shall also be required to present documentation from the local security office or ID card sponsor confirming that the ID card has been reported lost or stolen. **(T-0)** This documentation must be scanned and stored in DEERS. **(T-0)** For the dependents, the DD Form 1172-2 serves as the support documentation for a lost or stolen card…"

Table A10.1. Cardholder and SSM/VO/IO Actions.

Card holder will:	SSM / VO / IO will:
Lost – report loss to his /her security office or appropriate sponsor agency and request lost application, memorandum, counseling statement, or report. **(T-2)**	Accept lost application, memorandum, counseling statement, or report from card holder and scan into DEERS/RAPIDS. **(T-2)** See **Attachment 11** for sample memorandum.
Stolen – report theft to his /her security office or appropriate sponsor agency and request theft application, memorandum, or report. **(T-2)**	Accept theft application, memorandum, or report from card holder and scan into DEERS/RAPIDS. **(T-2)** See **Attachment 11** for sample memorandum.
Destroyed - report destruction to his /her security office or appropriate sponsor agency and request destruction application, memorandum, or report, unless damaged CAC is in possession of holder and presented to IO. **(T-2)**	Accept destruction application, memorandum, or report from card holder and scan into D/R. **(T-2)** See **Attachment 11** for sample memorandum.
Other – report confiscated, copied, forged, modified, or returned identity credential, etc., to his/her security office or appropriate sponsor agency and request application, memorandum, or report. **(T-2)**	Accept application, memorandum, or report and scan into DEERS/RAPIDS. **(T-2)** See **Attachment 11** for sample memorandum.

Attachment 11

SAMPLE MEMORANDUM LOST, STOLEN, DESTROYED IDENTITY CREDENTIAL – COMMON ACCESS CARD

Date

MEMORANDUM: Report of Lost, Stolen, Destroyed Identity Credential - Common Access Card.

TO: Real-time Automated Personnel Identification System ID Card Issuance Facility, Site Security Manager

FROM: See **Notes 1-10** below for each respective service / agency action.

1. Insert card holder First Name, Middle Initial, Last Name, reported his / her Common Access Card as lost/stolen/destroyed (circle one), in the vicinity of **insert location**, on or about **insert date**.

2. He/She (circle one) has been directed to return the Common Access Card, if found, to the nearest uniformed Services/Agency Real-time Automated Personnel Identification System facility.

3. Insert card holder Last Name has been advised of their responsibility to maintain control of Government Property in their possession, and the seriousness of possible compromise of physical and logical access security.

Respectfully,

Name
Title
Telephone number, email address (if available)

Notes:
(1) Coast Guard - When a signed incident report cannot be obtained by base security or the local police department, USCG CAC recipients must present a memorandum (in accordance with the above sample) on USCG letterhead and signed by the Commanding Officer or Officer-in-Charge.

(2) Air Force - CAC recipient must present a copy of the report filed with the installation security or local police; or a memorandum prepared (in accordance with the above sample) on USAF letterhead from the recipient's Commanding Officer, Officer-in-Charge, or Noncommissioned Officer for military, COR or Trusted Agent for contractors, and Supervisor/Division Chief for civilians.

(3) Space Force - CAC recipient must present a copy of the report filed with the installation security or local police; or a memorandum prepared (in accordance with the above sample) from

the recipient's Commanding Officer, Officer-in-Charge, or Noncommissioned Officer for military, COR or Trusted Agent for contractors, and Supervisor/Division Chief for civilians.

(4) Navy – CAC recipient must present a copy of the report filed with the installation security or local police; or a memorandum prepared (in accordance with the above sample) on Navy letterhead from the recipient's Commanding Officer, Officer-in-Charge, or Noncommissioned Officer for military, COR, and Supervisor /Division Chief for civilians.

(5) Marine Corps - CAC recipient must present a copy of the report filed with the installation security or local police; or a memorandum prepared (in accordance with the above sample) on Marine Corps letterhead from the recipient's Commanding Officer, Officer-in-Charge, or Noncommissioned Officer for military, COR, and Supervisor/Division Chief for civilians.

(6) Public Health Service – CAC recipient must present a signed copy of the incident report filed with the installation Security or Provost Marshall's office or local police. If an incident report cannot be obtained, a memo (in accordance with the above sample) from the individual's OIC, Division Chief, or Supervisor.

(7) National Oceanic and Atmospheric Administration - CAC recipient must present a copy of the report filed with the installation security or local police; or a memorandum prepared (in accordance with the above sample) on NOAA letterhead from the recipient's Commanding Officer, Officer-in-Charge for uniformed service personnel, COR, and Supervisor /Division Chief for civilians.

(8) Other Department of Defense/Federal and Non-Federal Agency Offices – refer to local lost/stolen / destroyed identity credential processing procedures.

(9) Local procedures apply when individual is not permanently assigned but is performing temporary duty, on leave, or official business.

(10) Mail all Common Access Cards to Defense Manpower Data Center, 1600 North Beauregard Street, Alexandria, VA 22311; 1-800-3-RAPIDS (1-800-372-7437), Defense Switch Network 698-5000 (country code 312).

Attachment 12

MISSION PARTNER IDENTITY, CREDENTIALING AND ACCESS MANAGEMENT, DEFENSE BIOMETRIC IDENTIFICATION SYSTEM, DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (DBIDS), DEFENSE NATIONAL VISITOR CENTER, DEFENSE CROSS-CREDENTIALING IDENTIFICATION SYSTEM, REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM SELF-SERVICE (RSS), AND COMMON ACCESS CARD PERSONAL IDENTITIFICATION NUMBER RESET PROGRAMS, VOLUNTEER LOGICAL ACCESS CREDENTIAL, MILCONNECT, ID CARD OFFICE ONLINE, NIPRNET ENTERPRISE ALTERNATIVE TOKEN SYSTEM PROGRAMS

A12.1. Mission Partner Identity, Credentialing and Access Management (MP-ICAM). MP-ICAM, (formerly TASS) will serve as the vehicle to establish a record into DEERS for eligible DoD and uniformed Services contractors and eligible non-DoD populations, in an effort to maintain the integrity of DEERS and to ensure physical and logical security in compliance with Homeland Security Presidential Directive-12 standards. **(T-2)** MP-ICAM is a web portal for the verification of contractors by Government Sponsors for the purpose of issuing CAC. MP-ICAM replaces the existing 1172-2 paper forms with a web interface and database for tracking the request process and updating DEERS with DoD contractor, federal agency personnel, and volunteer/intern population information required for CAC issuance. The system will also provide periodic re-verification of contractor, federal agency personnel and volunteer/intern population to ensure that information is current and individuals who are no longer authorized CAC do not remain active when not appropriate.

A12.1.1. Refer to uniformed Services and DoD Agencies Standard Operating Policies and Procedures, enhancing existing guidance listed in DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards*: ID Card Life-Cycle, and DMDC MP-ICAM User Guides.

A12.1.2. MP-ICAM is not designed for the purposes of tracking populations and is a registration and enrollment function of the DEERS program. Agencies or units seeking to track certain populations enrolled in DEERS must find other alternatives or means of accountability.

A12.2. Defense Biometric Identification System (DBIDS). DBIDS is a DoD identity authentication and force protection tool that is fully operational at selected military locations around the world. Developed by DMDC, DBIDS serves as a physical access control and critical property registration system, using barcodes and biometrics to identify cardholders. DBIDS implements the policies outlined in DoDI 5200.08 and DoDI 8520.02 and is an approved system. DBIDS is authorized to issue DoD identity credentials for those individuals needing physical access and not otherwise eligible for a CAC.

A12.2.1. As DoD's largest physical access control system, DBIDS uses fingerprints and, in some cases, hand geometry to accurately identify personnel entering military installations. This system is more secure and efficient for personnel entering a military installation than flashing an identification card at a guard who must then compare the picture on the identification card to the cardholder. In addition to validating identity CACs, DBIDS also verifies authorizations and assigns access privileges based on identity, affiliation, and the current threat level. Unlike the "flash pass" method, DBIDS reveals phony and expired

identification cards and anyone unauthorized to access military installations. DBIDS reveals individuals who are wanted, barred from the installation, or have other law enforcement alerts.

A12.3. Defense National Visitors Center. The Defense National Visitors Center is the system for DoD facilities to authenticate DoD CAC-carrying visitors using a web-based connection. Defense National Visitors Center is available to DoD law enforcement and force protection elements and is recognized as an approved system under DoDI 1000.25, *DoD Personnel Identity Protection (PIP) Program.*

A12.4. Defense Cross-Credentialing Identification System. The Defense Cross-Credentialing Identification System shall provide mutual authentication of issued identity CACs between participating Federal Agencies and private sector business partners. Use of a federated identity system for recognition of CAC shall strengthen the security of the DoD. Defense Cross-Credentialing Identification System is an approved system under the PIP program.

A12.5. Identification Card Office (IDCO). The IDCO replaced Real-time Automated Personnel Identification System Self-Service (RSS). Formerly the User Maintenance Portal/Post Issuance Portal (UMP/PIP), IDCO is designed to process CAC holder requests to update E-mail addresses, E-mail certificates, and add and update CAC applications. IDCO allows CAC users the option of performing these updates from the convenience of their own desktop instead of requiring them to queue at a RAPIDS issuance location. In addition to increasing CAC user convenience, the IDCO relieves organizations of the administrative burdens currently associated with processing CAC holder post-issuance requests. Most importantly, the IDCO accomplishes these goals without compromising the high level of security provided by current processes. See milConnect and identification Card Office Online.

A12.6. Credential Access Card Personal Identification Numbers Reset (CPR). CAC holders who forget their PIN or lock their CAC by entering an incorrect PINs three successive times need a convenient way to reset their PIN. The CAC PINs Reset system was developed as an alternative to the RAPIDS workstation. It provides a flexible, single-purpose system, for timely PIN reset capability for unlocking CACs and allows installations the flexibility to position CAC PINs Reset terminals to best support the needs of their CAC users. The CAC PINs Reset process requires the appointment of Trusted Agent Security Managers and CAC PINs Reset Trusted Agents (CTAs). Trusted Agent Security Managers are responsible for the overall management of CAC PIN Reset workstations under their purview. CTAs reset CAC PIN.

A12.7. Volunteer Logical Access Credential (VoLAC). USD (P&R) Memorandum, August 14, 2008, authorizes Department of Defense to initiate DEERS/RAPIDS as the platform for issuing logical access credentials to perform volunteer/intern duties. Refer to NIPRNet Enterprise Alternative Token System (NEATS). The credential is valid for three years, and will have DoD PKI certificates (identity, email encryption, email digital signing, and Personal Identity Verification Authentication) for authentication to DoD networks. **Note:** Government sponsors are responsible for ensuring vetting requirements have been met before credential issuance, including retrieval and revocation when the card expires or is no longer in use. Individuals who receive VoLAC access must agree in writing, e.g., digital signature on the DD Form 2842, to be subject to all DoD issuances that govern logical access. **Note**: VoLAC is transitioning to the NEATS.

A12.7.1. The volunteer or intern must:

A12.7.2. Be an authorized DoD volunteer (10 USC, Section 1588 as implemented in DoDI 1100.21) or student intern (5 USC, Section 3111). **(T-0) Note:** Refer to Agency and Service specific implementation guidance for other eligible populations affiliated with the VoLAC program.

A12.7.3. Require frequent access to a DoD network to perform their volunteer duties. **(T-0)**

A12.7.4. Be a US citizen. **(T-0)**

A12.7.5. Be registered in DEERS through the MP-ICAM, (formerly TASS). **(T-0)**

A12.7.6. Receive a favorable National Agency Check as required by DoDM 5200.2 for individuals requiring network access for Automated Data Processing (ADP)-III positions. **(T-0) Note:** A credential may be issued upon submission of the National Agency Check paperwork and upon favorable completion of the automated Federal Bureau of Investigation National Criminals History Check (fingerprint check).

A12.7.7. Be eligible for a DoD sponsored unclassified network account. **(T-0)**

A12.7.8. Agree to be photographed and have his/her fingerprints captured and stored in DEERS. **(T-0)**

A12.8. milConnect. DoD associates and beneficiaries (includes sponsors and family members), manage their personal data and benefits for the DEERS program. Individuals sign in to update personal information to the DoD Global Address (GA), or to check health care coverage, Post 9/11 transfer education benefits, including retrieving correspondence. The DS Logon credential accepted by milConnect, eBenefits, RAPIDS, TRICARE, and other DoD sites provides 24x7 answers to individual benefits questions.

A12.9. NPRNet Enterprise Alternative Token System. A centralized token management system for NIPRNet medium assurance certificates on alternate logon tokens for use cases to include groups, admins, roles, code signing, and individuals not authorized to receive a CAC. NEATS improves security by providing the PKI authentication credentials to replace username and password. It strengthens accountability across the NIPRNet by tracking access to these PKI credentials.