BY ORDER OF THE SECRETARIES OF THE AIR FORCE THE ARMY, THE NAVY, THE MARINE MARINE CORPS, HOMELAND SECURITY, COMMANDANT COMMERCE, HEALTH AND HUMAN NOAA CORPS SERVICES

AIR FORCE INSTRUCTION 36-3026, VOLUME 2
ARMY REGULATON (AR) 600-8-14
BUPERS INSTRUCTION1750.10C
CORPS ORDER (MCO) 5512.11E
INSTRUCTION M5512.1B
DIRECTIVES, CHAPTER 1, PART 5
COMMISSIONED CORPS MANUAL 29.2
INSTRUCTIONS 1 AND 2

17 MAY 2018

Personnel

COMMON ACCESS CARD (CAC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: AF/A1P

Certified by: SAF/MRM
(Mr. Jeffrey R. Mayo)
Pages: 102

This is a first publication issue of Volume 2 and provides new guidance for Identification card issuing facilities supported by the Real-time Automated Personnel Identification System and the Defense Enrollment Eligibility Reporting System. Volume 2 supports the ID card issuance lifecycle, including the administration of ID card benefits and privileges as listed in AFI 36-3026, Volume 1, *Identification Cards For Members of The Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel.* All uniformed Services Real-time Automated Personnel Identification System sites are required to maintain a printed copy of this inter-service instruction AFI 36-3026, Volume 2 in case of emergencies as well as for informational and training purposes according to paragraph 1.3, Cross-Servicing Agreement. This inter-service publication implements Department of Defense Manual 1000.13, Volume 1, *DoD Identification*

(ID) Cards: ID Card Life-Cycle, January 23, 2014 and Volume 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, January 23, 2014, DoD Instruction (DoDI) *1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, January 23, 2014, Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004; Department of Defense Directive 1000.25, *DoD Personnel Identity Protection (PIP) Program*, July 19, 2004; Federal Information Processing Standards Publication 201 (FIPS-201), Personal Identity Verification of Federal Employees and Contractors; Department of Commerce, National Institute of Standards and Technology, Special Publication 800-73, Interfaces for Personal Identity Verification;" National Institute of Standards and Technology Special Publication 800-76, Biometric Data Specifications for Personal Identity Verification; Department of Commerce, National Institute of Standards and Technology, Special Publication 800-79, Guidelines for the Certification and Accreditation (C&A) of Personal Identity Verification Card Issuing Organizations; Department of Defense Directive 8190.3, *Smart Card Technology*, August 31, 2002; DoDI 1000.01, *Identity Cards Required by the Geneva Conventions*, April 16, 2012; DoDI 1000.23, *Department of Defense Civilian Identification (ID) Card*, December 10, 1998; DoDI 1341.2, *Defense Enrollment Eligibility Reporting System Procedures*, March 19, 1999; and DoD Directive 1000.22, *Uniformed Services' Identification (ID) Cards*, October 8, 1997; Department of Defense Directive 1330.9, *Armed Services Exchange Regulations*, November 27, 2002; Department of Defense Directive 1341.1, *Defense Enrollment Eligibility Reporting System*, May 21, 1999; Department of Defense Directive 8190.3, *Smart Card Technology*, August 31, 2002, Department of Defense Directive 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003, and DoDI 8910.1M, *Department of Defense Instruction for Information Collection and Reporting*, May 19, 2014. Additionally, this inter-service publication supports the Defense Enrollment Eligibility Reporting System and the Real-time Automated Personnel Identification System for the Army, Navy, Air Force, Marine Corps, Coast Guard, the Commissioned Corps of the National Oceanic and Atmospheric Administration, United States Public Health Service, National Guard, and U.S. 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 Card 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 Common Access Card of the Uniformed Services, Department of Defense Components and other eligible recipients. This publication provides procedures for compliance of forms prescribed in the DoD Real-time Automated Personnel Identification System Workstation and Verifying Official (VO) Certification Practice Statement, herein referred to as the Real Time Automated Personnel Identification System/VO Certification Practice Statement. This publication implements DD Form 2841, DoD *Public Key Infrastructure (PKI) Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities*, DD Form 2842, *DoD PKI Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities*, DD

Form 1172-2, *Application for Department of Defense CAC DEERS Enrollment*, and DD Form 577, *Appointment/Termination Record-Authorized Signature*.

This publication implements Air Force Policy Directive (AFPD) 36-30, *Military Entitlements,* DoDI 1000.1, *Identity Cards Required by the Geneva Conventions, January 30, 1974 with Changes 1 and 2, 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, December 5, 1997, 1341.2, *Defense Enrollment Eligibility Reporting System Procedures*, March 19, 1999; It supports the Defense Enrollment Eligibility Reporting System and the Real-time Automated Personnel Identification System for the Army, Navy, Air Force, Marine Corps, Coast Guard, the National Oceanic and Atmospheric Administration, Commissioned Officer Corps, United States Public Health Service, National Guard, and U.S. Armed Forces Reserve. This instruction applies to Regular Air Force (RegAF), Air Force Reserve (AFR) and Air National Guard personnel, except where noted otherwise. This publication also includes instructions applying to Air Force Real-time Automated Personnel Identification System facilities (RegAF, Air Force Reserve (AFR), and Air National Guard), identifying Tier waiver authorities (T-0, T-1, T-2, and T-3) as approved by the Air Force Inspector General Advisory Board. This inter-service publication is available at http://www.e-publishing.af.mil. Use this instruction to prepare issue, use, account for, and dispose of ID cards the Uniformed Services issue. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, 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.

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.

The Privacy Act of 1974 affects this publication. This Instruction requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Chapter 55 Medical and Dental Care (Sections 3013 for the Army, 5013 for the Navy, 8013 for the Air Force); Title 33 United States Code, 857a, (National Oceanic and Atmospheric Administration) Executive Order No. 11023 (National Oceanic and Atmospheric Administration); and Executive Order (EO) 9397, as amended. The applicable System of Records Notice Defense Manpower Data Center, 02 DoD, Defense Enrollment Eligibility Reporting System is (are) available at:
http://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/627618/dmdc-02.dod.aspx.

The Paperwork Reduction Act of 1995 affects this instruction. See attachment 1 for glossary. Process supplements that affect any military personnel function as shown in AFI 33-360, *Publications and Forms Management*. This publication may not be supplemented.

Refer commended changes and questions about this publication to HQ AFPC/DP3SA using the AF Form 847, *Recommendation for Change of Publication* route AF Form 847 from the field through the appropriate functional chain of command.

Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW the Air Force Records Disposition Schedule in the Air Force Records Information Management System.

The OPR will not process any waivers to this publication. Refer to attachment 1 for Glossary of References and Supporting Information.

Chapter 1—**COMMON ACCESS CARD--GENERAL GUIDELINES**

Chapter 1

COMMON ACCESS CARD--GENERAL GUIDELINES

1.1. General Guidelines. The Department of Defense Common Access Card meets the Federal requirements for credentialing contained within Homeland Security Presidential Directive-12 and Federal Information Processing Standards Publication 201-1 and 201-2. Refer DoDI 1000.13, Volume 1, January 23, 2014, *DoD Identification Cards*: ID Card Life-Cycle.

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

1.1.2. This inter-service instruction also applies to the Commissioned Corps of the U.S. Public Health Service, under agreement with the Department of Health and Human Services; and the National Oceanic and Atmospheric Administration, under agreement with the Department of Commerce.

1.2. Identity Proofing and Vetting.

1.2.1. Common Access Card eligible individuals will not be issued a Common Access Card without first satisfying the background vetting requirements in according 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, August 5, 2005. Initial issuance of a Common Access Card requires, at a minimum, the completion of Federal Bureau of Investigation fingerprint check with favorable results and submission of a National Agency Check with Inquiries to the Office of Personnel Management, or a Department of Defense-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. List of Department of Defense Investigations.

Investigation Type	JPAS Code	NACI Equiv	Description
ANACI	AN	Yes	Access National Agency Check plus Written Inquires & Credit Check
BGI-0112	37	Yes	Upgrade Background Investigation (1-12 months from LBI)
BGI-1336	27	Yes	Upgrade Background Investigation (13-36 months from LBI)
BGI-3760	29	Yes	Upgrade Background Investigation (37-60 months from LBI)
BI	4	Yes	Background Investigation
BIPN	P	Yes	Background Investigation + Current National Agency Check
BIPR	G	Yes	Periodic Reinvestigation of Background Investigation
BI	4	Yes	Background Investigation

Investigation Type	JPAS Code	NACI Equiv	Description
BIPN	P	Yes	Background Investigation + Current National Agency Check
BIPR	G	Yes	Periodic Reinvestigation of Background Investigation
Investigation Type	**JPAS Code**	**NACI Equiv**	**Description**
BI	4	Yes	Background Investigation
BIPN	P	Yes	Background Investigation + Current National Agency Check
BIPR	G	Yes	Periodic Reinvestigation of Background Investigation
BITN	F	Yes	Background Investigation (10 year scope)
CNAC	CN	Yes	National Agency Check plus Credit Check
CNCI	CC	Yes	Child Care National Agency Check plus Written Inquires and Credit Check [CNACI in OPM Components]
IBI	9	Yes	Interview Oriented Background Investigation
LBI	K	Yes	Limited Background Investigation
LBIP	R	Yes	Limited Background Investigation plus Current National Agency Check
LBIX	Y	Yes	Limited Background Investigation — Expanded
MBI	L	Yes	Minimum Background Investigation
MBIP	Q	Yes	Minimum Background Investigation plus Current National Agency Check
MBIX	X	Yes	Minimum Background Investigation — Expanded
NACB	D	Yes	National Agency Check/National Agency Check plus Written Inquires & Credit Check plus Background Investigation Requested
NACI	3	Yes	National Agency Check plus Written Inquires and Credit Check
NACL	7	Yes	National Agency Check plus Special Investigative Inquiry
NACLC	XX	Yes	National Agency Check, Local Agency Check & Credit Check
NACP	6	Yes	National Agency Check plus 10 Years Service
NACS	E	Yes	National Agency Check/National Agency Check plus Written Inquires & Credit Check plus Single Scope B.I. Requested
NACW	C	Yes	National Agency Check plus Written Inquires & Credit Check
NACZ	Z	Yes	National Agency Check plus Written Inquires and Credit Check plus Special Investigative Inquiry
NLC	XX	Yes	National Agency Check, Local Agency Check & Credit Check
NNAC	N	Yes	National Agency Check plus Written Inquires and Credit Check Plus Current National Agency Check
NPSB	H	Yes	National Agency Check plus Partial Special Background Investigation
PPR	19	Yes	Phased Periodic Reinvestigation
PRI	11	Yes	Periodic Reinvestigation
PRS	#	Yes	Periodic Reinvestigation — Secret
PRSC	PR	Yes	Periodic Reinvestigation — Secret/Confidential
PTSBI	35	Yes	Public Trust Special Background Investigation
SBBI	S	Yes	Special Background Investigation plus Current Background Investigation
SBI	5	Yes	Special Background Investigation

Investigation Type	JPAS Code	NACI Equiv	Description
SBIP	M	Yes	Special Background Investigation/Single Scope Background Investigation plus Current National Agency Check
SBPR	J	Yes	Periodic Reinvestigation of Special Background Investigation/Single Scope Background Investigation
SSBI	0	Yes	Single Scope Background Investigation
CI	I	No	Character Investigation
ENAC	1	No	Entrance National Agency Check
ENAL	8	No	Entrance National Agency Check plus Special Investigative Inquiry
LRCN	B	No	Local Records Checks plus Investigation Requested
NAC	2	No	National Agency
NACFI	48	No	Non-Appropriated Fund Suitability Determination
NSI	46	No	NSI — National Agency Check with Inquiries /Suitability Determination
OTHR	U	No	Information Furnished by Sources Other than a Listed Investigation
RSI	43	No	Reimbursable Suitability/Security Investigation
SAC	92	No	Single Agency Check/Special Agreement Check
SBIR	V	No	Single Scope Background Investigation Requested
SII	O	No	Special Investigative Inquiry
XNAC	A	No	Expanded National Agency Check/Entrance National Agency Check

1.2.2. ID cards must be issued to the Common Access Card 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 Common Access Card issuance process, all personnel shall present two forms of ID in original form to verify a claimed identity. 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. **Note:** Refer to Department of Homeland Security U.S. Citizenship and Immigrations Services, Form I-9, Office of Management and Budget No 1615-0047, Employment Eligibility Verification and Lists of Acceptable Documents http://www.uscis.gov/ in reference to identity proofing for Defense Enrollment Eligibility Reporting System enrollment, and identification card issuance. The Form I-9 will be used as an Identity Documentation reference list only. Consistent with applicable law, at least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture identification. The identity documents will be inspected for authenticity and scanned and stored in the Defense Enrollment Eligibility Reporting System according to the Real-time Automated Personnel Identification System User Guide upon issuance of an identification. The photo identification requirement cannot be waived, consistent with applicable statutory requirements. **(T-0).**

1.2.4. In the future, Real-time Automated Personnel Identification System sites will have the capability to verify the background vetting processes have been initiated and/or successfully completed from Department of Defense or from a Federal Government authoritative data source. Once this capability is in place, any Common Access Card applicant who is identified in Real-time Automated Personnel Identification System 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.

1.3. Purpose of the Common Access Card. The Common Access Card is the ID card 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. Coast Guard 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) and paragraphs 1.5 – 1.5.1. The Common Access Card 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. The Common Access Card also will be used to facilitate standardized, uniform access to Department of Defense facilities, installations, and computer systems (See paragraphs 1.3.1 – 1.3.3). **Note:** For those individuals not eligible for a Common Access Card, but requiring physical access, 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. This population, if eligible, will continue to use Department of Defense ID cards pursuant to Department of Defense Instruction 1000.13 Volume 1, Enclosure 2, until they are migrated to an applicable new card (refer to Chapter 2 within this instruction).

1.3.1. The Common Access Card shall be used to facilitate standardized, uniformed access to Department of Defense facilities, installations, and computer systems by:

1.3.1.1. Service as the Geneva Conventions Card under Article 17 and/or an ID and privilege card, as appropriate, for eligible categories; relative to the Treatment of Prisoners of War of August 12, 1949.

1.3.1.2. Being the principal card facilitating physical access to buildings, facilities, installations and controlled spaces.

1.3.1.3. Being the primary platform for the public key infrastructure authentication token used to access Department of Defense computer networks and systems in the unclassified environment.

1.3.2. Real-time Automated Personnel Identification System Self-Service Portal. The RSS Portal allows eligible populations to self-service on certain actions such as update information in Defense Enrollment Eligibility Reporting System; add/change E-mail address to receive initial or new E-mail and E-mail certificates, add a Personnel Category Code to the User Principle Name of the E-mail Signature Certificate, Activate the Personal Identity Verification Authentication Certificate, download applications, and view/update contact information at https://www.dmdc.osd.mil/self_service.

1.3.3. RSS Portal allows Common Access Card recipients verify a family member's relationship and eligibility by digitally signing the DD Form 1172-2 for identification card reissuance. See AFI 36-3026, Volume 1, Chapter 1 for RSS Portal.

1.4. Common Access Card Issuance Platform. The Common Access Card is generated by the Real-time Automated Personnel Identification System, an application of the Defense Enrollment Eligibility Reporting System.

1.4.1. Authoritative Data Source. According to USD (P&R) Memorandum, *DEERS/RAPIDS*

Lock Down for Contractors, November 10, 2005 *and DEERS/RAPIDS Lock Down for Additional Populations,* October, 29, 2010. Memorandums codified in DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* January 23, 2014. Common Access Card eligible personnel must be registered in Defense Enrollment Eligibility Reporting System through either an authoritative personnel data feed from the appropriate Service or Agency, or through the Trusted Associate Sponsorship System, formerly, Contractor Verification System.

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

1.4.3. The Common Access Card is worn 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. The Armed Forces of the United States Geneva Conventions identification Card will be issued to members of the Active Component, Selected Reserve, Participating Individual Ready Reserve, Armed Forces Health Professions Financial Assistance Program, contracted members (cadet or Midshipman) of the Reserve Officer Training Corps, and others on active duty for 31 days or more. For members of the National Oceanic and Atmospheric Administration and the U.S. Public Health Service "Armed Forces" will be modified to state "Uniformed Services." The United States Department of Defense/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces will be issued to all Emergency-Essential employees, contingency contractor employees, and civilian noncombatant personnel (including both appropriated fund and non-appropriated fund employees) who are deployed in conjunction with military operations overseas. The United States Department of Defense/Uniformed Services identification and Privilege Card will be issued to sponsors eligible for a Common Access Card, other than current or retired members of the Uniformed Services, who are eligible for Uniformed Services benefits and privileges. The United States Department of Defense/Uniformed Services identification Card will be issued to Department of Defense civilian employees (including both appropriated fund and non-appropriated fund employees) and eligible contractor employees.

1.5.1. Common Access Card eligibility for other populations, including Department of Defense contractors, non-Department of Defense Federal civilians, State employees, and other non-Department of Defense affiliates is based on the Department of Defense government sponsor's determination of the type and frequency of access required to Department of Defense facilities or networks that will effectively support the mission. To be eligible for a Common Access Card**,** the individual must require:

1.5.1.1. Access to multiple Department of Defense facilities or access to multiple non-Department of Defense Federal facilities on behalf of the Department on a recurring basis for a period of 6 months or more (this requirement is applicable to Department of Defense contractors only).

1.5.1.2. Access to both a Department of Defense facility and access to Department of Defense networks on site or remotely.

1.5.1.3. Remote access to Department of Defense networks that use only the Common Access Card logon for user authentication.

1.5.1.4. Surviving Family Members -upon request, next of kin may obtain the Common Access Card for an individual who has perished in the line of duty. All Common Access Cards 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.

1.6. Canceled Cards. The Common Access Card replaces certain manually prepared and Uniformed Services ID (formerly referred to as "Teslin" cards) for Common Access Card eligible populations. Table 1.2 lists the cards which are or may be replaced by the Common Access Card. Table 1.3 lists the cards which are or may be replaced by the plastic Department of Defense/uniformed Services Civilian Retiree ID Card. **Note:** Certain manually prepared identification cards are cancelled per USD (P&R) Memorandum, *"Cancellation of Manually Produced Identification (ID) Cards,"* October 29, 2010.

1.6.1. The Services Academies will issue 4-year Common Access Card with a 3-year Public Key Infrastructure certificate. **Note:** If an individual is not eligible for Common Access Card, refer to AFI 36-3026 IP, *Identification Cards For Members of The Uniformed Services, Their Eligible Family Members, And Other Eligible Personnel,* Volume I for qualifying criteria, e.g. DD Form 1934. The manual DD Form 1934 is not obsolete and will remain in inventory until further notice.

Table 1.2. The Common Access Card Replaces:

FORM	TITLE	TYPE OF ISSUE
DD Form 2ACT	Armed Forces of the United States Identification Card (Active)(Green)	Manually prepared (canceled)
DD Form 2ACT	Armed Forces of the United States Geneva Conventions Identification Card (Active) (Green)	Machine-readable USID card
DD Form 2ACT	Armed Forces of the United States Identification Card (Active)(Green)	Manually prepared (canceled)
DD Form 2ACT	Armed Forces of the United States Geneva Conventions Identification Card (Active) (Green)	Machine-readable USID card
DD Form 2RES	Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)	Machine-readable USID card
DD Form 489	Geneva Conventions Identity Card for Civilians Who Accompany the Armed Forces	Manually prepared (canceled)
DD Form 2574	Exchange Service Identification and Privilege Card	Manually prepared
DD Form 2750	Department of Defense Civilian Identification Card	Machine-readable non- USID card)
DD Form 2764	United States Department of Defense/Uniformed Services Civilian Geneva Conventions Identification Card (Tan)	Machine-readable USID card
DD Form 2765	Department of Defense /Uniformed Services Identification and Privilege Card (Tan)	Machine-readable USID card

Note: The manual DD Form 2574, Exchange Service Identification and Privilege Card is pending migration to the DEERS/Real Time Automated Personnel Identification System (D/R) platform.

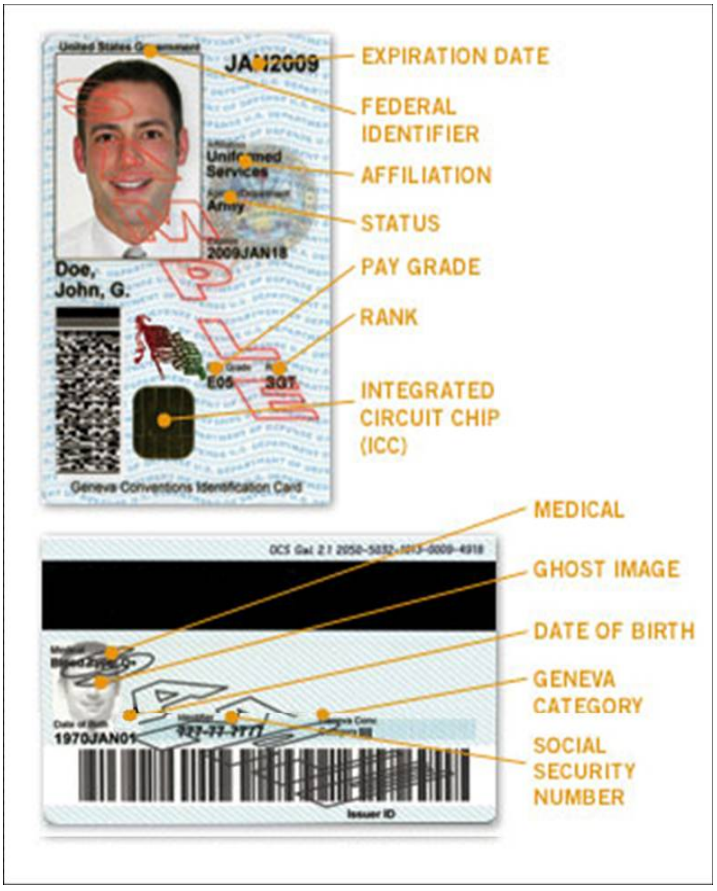
Table 1.3. The Plastic Non-Chip Card Replaces:

DA Form 1602	Civilian Identification Card	Manually prepared
AF Form 354	Civilian Identification Card	Manually prepared (canceled)

1.7. Types of Common Access Cards. There are four Common Access Card types used within the Department, based on cardholder eligibility. See Figures 1.1, 1.2, 1.3, and 1.4.

1.7.1. Armed Forces of the United States, Geneva Conventions Identification Card, see Figure 1.

Figure 1.1. Armed Forces of the United States Geneva Conventions ID Card.



1.7.1.1. The Armed Forces of the United States Geneva Conventions identification Card is the primary identification, physical, and logical access card for the following: Members on active duty for 31 consecutive days or more, Selected Reserve members, Participating Individual Ready Reserve members attached to a unit for retirement point purposes, Armed Forces Health Professions Financial Assistance Program members, contracted members (cadet or Midshipman) of the Reserve Officer Training Corps, National Guard members, including the National Oceanic and Atmospheric Administration and the U.S. Public Health Service. This card shall be used for access to Department of Defense facilities and systems access, serve as the member's Geneva Conventions identification card, and identify the member's eligibility for benefits and privileges administered by the Uniformed Services. **Note:** Refer to AFI 36-3026, Volume 1, Table 1.17, Tables A2.39 and A2.45 for National Oceanic and Atmospheric Administration Wage Mariner populations for entitlements to benefits and privileges. Wage Mariner members may qualify for either the Identity Common Access Card or Identity and Privilege Common Access Card within this instruction, and their family members may qualify for the DD Form 1173 according to Volume 1.

1.7.1.2. In the Status area of the card, the card will show the affiliation of "Uniformed Services" (formerly Military) for members on active duty, and for members of the Selected Reserve not on active duty or full-time National Guard duty for 31 days or more.

1.7.1.3. Armed Forces of the United States Geneva Conventions Identification Card. This is the primary identification card for Active Uniformed Services members, Selected Reserve members, National Guard members, and Individual Ready Reserve members in a training capacity (voluntary training units), as well as military members of the Coast Guard, National Oceanic and Atmospheric Administration, and U.S. Public Health Service. It identifies the member's eligibility for benefits and privileges administered by the Uniformed Services.

1.7.1.4. The affiliation area of the card will state "Uniformed Services" and the status area of the card will reflect the member's sponsoring Service, Agency, or Department. The status of the individual will be located electronically within the card's Integrate Circuit Chip (Active, Reserve, National Guard). It is necessary that this chip be updated when status changes occur e.g., mobilization, Reserve on an active duty.

1.7.1.5. The next generation Common Access Card does not change current benefits and entitlements, or the requirement to update the Defense Enrollment Eligibility Reporting System when any changes to a member's family, status, or other information changes.

1.7.1.6. DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Reserve), machine-readable card will continue to be issued to those Reserve Component categories not eligible for the Common Access Card e.g., Non-participating Individual Ready Reserve (not including Armed Services Health Professions Financial Assistance Program members, and Reserve Officer Training Corps cadets and midshipmen), standby Reserve, and inactive National Guard.

1.7.1.7. DD Form 1934, *Geneva Conventions Identity Card for Medical and Religious Personnel* who Serve in/or Accompany the Armed Forces, remains valid and will continue to be issued according to Department of Defense Instruction 1000.1.

1.7.1.8. If a member is deployed and there are no network communications either with Defense Enrollment Eligibility Reporting System or the Certificate Authority, 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 Infrastructure certificates and must be replaced as soon as the member can reach a Real-time Automated Personnel Identification System workstation or when network communications have been restored to Defense Enrollment Eligibility Reporting System.

1.7.2. U.S. Department of Defense/Uniformed Services Geneva Conventions identification for Civilians Accompanying the Armed Forces, see Figure 1.2.

Figure 1.2. U.S. Department of Defense/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces.

1.7.2.1. The U.S. Department of Defense/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces serves as the United States Department of Defense and/or Uniformed Services Geneva Conventions identification card

for civilians accompanying the Armed Forces and shall be issued according to Department of Defense Instruction 1000.1.

1.7.2.2. This card shall be the primary identification card for: (1) Emergency-essential employees as defined in Department of Defense Directive 1404.10, (2) Contingency contractor employees as defined in Department of Defense Instruction 3020.41 and (3) Civilian noncombatant personnel who have been authorized to accompany U.S. military forces in regions of conflict, combat, and contingency operations and liable to capture and detention by the enemy as prisoners of war.

1.7.2.3. This Common Access Card replaces the DD Form 489, *Geneva Conventions Identity Card* for *Persons who Accompany the Armed Forces*, and some uses of the current DD Form 2764, United States Department of Defense and/or Uniformed Services Civilian Geneva Conventions identification Card.

1.7.2.4. DD Form 1934 remains valid and continues to be issued according to Department of Defense Instruction 1000.1.

1.7.2.5. Eligible individuals permanently assigned in foreign countries for at least 365 days (excluding local nationals are in their home country, not a foreign country) will have the word “OVERSEAS” printed within the authorized patronage area of the Common Access Card.

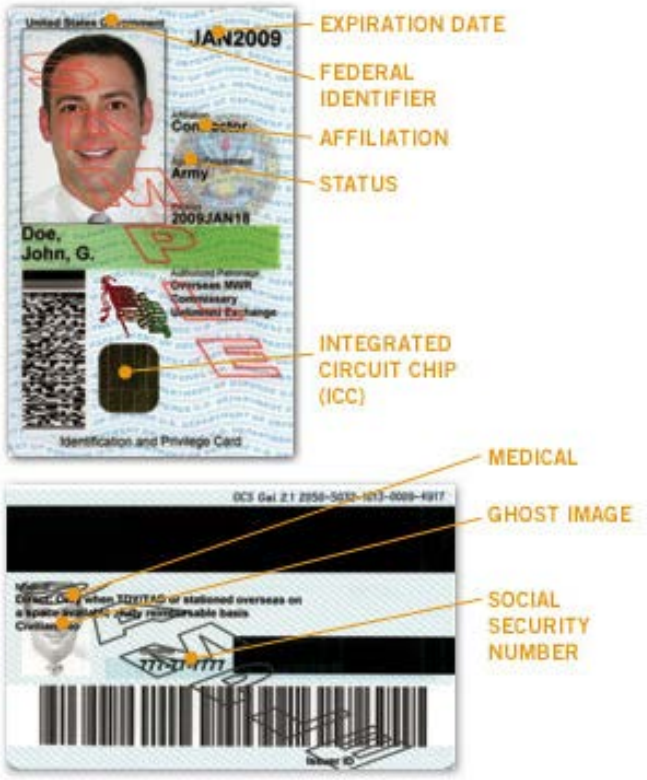
1.7.2.6. The authorized patronage area for eligible individuals permanently assigned within the continental United States will be blank. Travel orders authorize access for these individuals while enroute to the deployment site.

1.7.2.7. During a conflict, combat, or contingency operation, civilian employees with a U.S. Department of Defense/Uniformed Services Geneva Conventions identification card for civilians accompanying the Armed Forces will be granted all commissary, exchange, and medical privileges available only at the site of the deployment, regardless of the statements on the identification card. Contractor employees possessing this Common Access Card shall receive the benefit of those commissary, exchange, Morale, Welfare, and Recreation, and medical privileges that are accorded to such persons by international agreements in force between the United States and the host country concerned and their letter of authorization.

1.7.2.8. The medical area on the card for individuals on permanent assignment in a foreign country will contain a statement, "When TAD/temporary duty or stationed overseas on a space-available fully reimbursable basis."

1.7.3. U.S. Department of Defense and/or Uniformed Services Identification and Privilege Card, see Figure 1.3.

Figure 1.3. U.S. DoD and/or Uniformed Services ID and Privilege Card.



1.7.3.1. The U.S. Department of Defense and/or Uniformed Services identification and Privilege Card replaces the DD Form 2765, *Department of Defense and Uniformed Services Identification and Privilege Card*, and DD Form 2574, *Exchange Service Identification and Privilege Card*. Publication of these forms is no longer authorized. The Common Access Card is the primary identification card granting benefits and privileges for civilian employees, contractors, and foreign national military, as well as other eligible personnel to the following categories:

1.7.3.1.1. Department of Defense and Uniformed Services civilian employees (both appropriated and non-appropriated fund) when required to reside in a household on a military installation within the continental United States, Hawaii, Alaska, Puerto Rico, and Guam.

1.7.3.1.2. Department of Defense and Uniformed Services civilian employees when stationed or employed and residing in foreign countries for a period of at least 365 days.

1.7.3.1.3. Other U.S. Government agency civilian employees when stationed or employed and residing in foreign countries for a period of at least 365 days.

1.7.3.1.4. Department of Defense contractors when stationed or employed and residing in foreign countries for a period of at least 365 days.

1.7.3.1.5. Department of Defense Presidential appointees who have been appointed with the advice and consent of the Senate. These Presidential 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.

1.7.3.1.6. Civilian employees of the Army and Air Force Exchange System, Navy Exchange System, Marine Corps Exchange System, and non-appropriated fund activity employees of the Coast Guard Exchange Service. Exchange employees are entitled to all privileges of the exchange system, except for purchase of articles of uniform and state tax-free items.

1.7.3.1.7. Uniformed and non-uniformed full-time paid personnel of the Red Cross assigned to duty with the Uniformed Services within the continental United States continental United States, Hawaii, Alaska, Puerto Rico, and Guam, when required to reside in a household on a military installation.

1.7.3.1.8. Uniformed and non-uniformed, full-time, paid personnel of the Red Cross assigned to duty with the Uniformed Services in foreign countries.

1.7.3.1.9. Foreign national military who meet the eligibility requirements in the following categories:

1.7.3.1.10. Active Duty officer and enlisted personnel of North Atlantic Treaty Organization and Partnership For Peace countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department.

1.7.3.1.11. Active Duty officer and enlisted personnel of non-North Atlantic Treaty Organization countries serving in the United States under the sponsorship or invitation of the Department or a Military Departments.

1.7.3.1.12. Active Duty officer and enlisted personnel of North Atlantic Treaty Organization and non-North Atlantic Treaty Organization countries when serving outside the United States and outside their own country under the sponsorship or invitation of the Department 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 U.S. military establishment.

1.7.4. U.S. Department of Defense/Uniformed Services identification Card. U.S. Department of Defense/Uniformed Services Identification Card, see Figure 1.4.

Figure 1.4. U.S. Department of Defense/Uniformed Services ID Card.

1.7.4.1. This U.S. Department of Defense/Uniformed Services identification Card shall be the primary identification card for eligible civilian employees, contractors, and foreign national affiliates who do not receive the identification and privilege Common Access Card.

1.7.4.2. Department of Defense civilian employees are automatically eligible for this Common Access Card, including:

1.7.4.2.1. Individuals appointed to appropriated fund and non-appropriated fund positions (to include civilian employees of the U.S. Coast Guard and National Oceanic and Atmospheric Administration).

1.7.4.2.2. Permanent or time-limited employees on full-time, part-time, or intermittent work schedules for 6 months or more. **Note:** There is no minimum time of employment required for Common Access Card issuance.

1.7.4.2.3. Senior Executive Service, Competitive Service, and Excepted Service employees.

1.7.4.3. The following personnel are eligible for this Common Access Card based on the Department of Defense/Uniformed Service Government sponsor's determination of the type and frequency of access required to Department of Defense facilities or networks:

1.7.4.3.1. Civilian employees, including: (1) Civilian employees of other Federal agencies working in support of the Department of Defense (including U.S. Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service), (2) State employees working in support of the National Guard, and (3) Intergovernmental Personnel Act employees.

1.7.4.3.2. Department of Defense contractors (including U.S. Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service).

1.7.4.3.3. Foreign national affiliates who meet the eligibility requirements include:

1.7.4.3.4. Foreign National Direct and Indirect Hires. Non-U.S. citizens hired under an agreement with the host nation and paid directly by the U.S forces (direct hire) or paid by an entity other than the U.S. forces for the benefits of the U.S. forces (indirect hire).

1.7.4.3.5. Foreign National Military, Civilians, and Contractors. Non-U.S. citizens who are sponsored by their government as part of an official visit or assignment to work on a Department of Defense facility and/or require access to Department of Defense networks both on site or remotely (remote access must be on an exception only basis for this category). These individuals are not paid or provided benefits under any arrangement with the United States.

1.8. Common Access Card Eligibility For Department of Defense Contractors, Non-DoD Federal Civilians, State Employees, And Other Non-DoD Affiliates. Common Access Card eligibility is based on the Department of Defense/Uniformed Service Government sponsor determination of the type and frequency of access required to Department of Defense facilities or networks that will effectively support the mission.

1.9. Temporary Credential for Deployed Personnel. On a limited basis for individuals (military, civilian, and contractor) who are deployed/mobilized, and needing a Common Access Card, an off-line card is provided (for the purposes of Geneva Conventions) when there are no network communications either with the Defense Enrollment Eligibility Reporting System database or the Department of Defense CA. The temporary card appearance will be the same as reflected in Figures 1.1, 1.2, 1.3, and 1.4, except there will be a white space where the Integrate Circuit Chip is normally located.

1.10. Expiration Dates. The Common Access Card 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 Department of Defense, whichever is earlier. Services Academies will issue 4-year Common Access Card with a 3-year Public Key Infrastructure certificate. For contractors, Common Access Cards will be issued for three years or the duration of the contract, not to exceed a three year time period per the Trusted Associate Sponsorship System (formerly Contractor Verification System), enrollment transaction to Defense Enrollment Eligibility Reporting System. See paragraph 1.13.

Table 1.4. 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 Department of Defense 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 Department of Defense or upon termination of the entitlement condition. See Attachment 2, including termination of benefits & privileges when authorized according to this instruction and AFI 36-3026, Volume 1.
United States DoD/Uniformed Services Identification and Privilege Card	

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

1.12. Reissuance. The Common Access Card 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. **Note:** Individuals are allowed to apply for a Common Access Card renewal starting 90 days prior to their expiration of a valid identification.

1.12.1. Reissue Common Access Card in accordance with AFI 36-3026(I), 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.

1.12.2. Initial Issue and Reissue. Provide and explain to the Common Access Card recipient that their signature on the DD Form 2842, (Subscriber) Certificate Acceptance and Acknowledgement of Responsibilities, acknowledges reading and accepting their responsibilities and obligations as stated on the form. Refer to AFI 36-3026(I), Volume 1, Chapters 12, 13, 15, 17, 18, and Service unique requirements.

1.13. Confiscating Common Access Cards. Common Access Cards are property of the U.S. Government. When a Common Access Card 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 1.5 may confiscate Common Access Cards under the following conditions:

Table 1.5. 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 Common Access Card has expired. A Common Access Card is being fraudulently used. A Common Access Card is presented by a person not entitled to its use. A Common Access Card is mutilated or illegible.
Senior Installation Officials.	Shoplifting is involved. The Senior installation official determines when to confiscate Common Access Cards. Senior installation officials, installation security authorities and installation legal staffs establish written base policy for confiscating Common Access Card 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.	Common Access Card recipients of any Service have cards that are mutilated so that their use as a Common Access Card is questionable. The Common Access Card has expired, altered, or an ineligible person.

1.13.1. Notify the installation security authorities immediately after having confiscated a Common Access Card or if involved in a situation requiring confiscation of a Common Access Card.
1.13.2. 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.
1.13.3. Installation security authorities provide the parent Service all information pertaining to the situation when the confiscated card belongs to a member of another Service.
1.13.4. Give a receipt or letter to the cardholder when confiscating a Common Access Card.

1.13.5. Return confiscated Common Access Cards immediately to the nearest Real-time Automated Personnel Identification System site with the reason for confiscation.

1.14. Retrieval /Disposition of the Common Access Card. Common Access Cards confiscated or turned in as invalid, inaccurate, inoperative, or expired shall be returned to a Real-time Automated Personnel Identification System site for disposition in accordance with Attachment 9 of this instruction and the Real-time Automated Personnel Identification System User Guide. **(T-0)**.

1.14.1. The Common Access Card is the property of the U.S. Government, shall be in the personal custody of the member at all times. Upon termination of employment, retirement or death, the Common Access Card must be recovered. **Note:** All recoverable Common Access Cards will be returned to Defense Manpower Data Center for accountability from the Real-time Automated Personnel Identification System facility. **Exception:** Upon request, next of kin may obtain the Common Access Card for an individual who has perished in the line of duty. All Common Access Cards 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.

1.14.2. Common Access Card - eligible populations will follow local in/out-processing procedures that include revoking the Common Access Card certificates for inter-departmental employment changes, relocations, etc. This also includes updating the Public Key Infrastructure email encryption and digital signature. Individuals being transferred within the Department, including mobilization must ensure their Defense Enrollment Eligibility Reporting System records pertaining to the Common Access Card are updated to Defense Enrollment Eligibility Reporting System. This record action is accomplished by the appropriate Service/Agency to Defense Enrollment Eligibility Reporting System. **Note:** Certificate maintenance is available by the Real-time Automated Personnel Identification System Self-Service web application (formerly User Maintenance Portal/Post Issuance Portal [UMP/PIP] system) to assist individuals with accomplishing Integrate Circuit Chip updates outside of the Real-time Automated Personnel Identification System environment.

1.15. Cross-Servicing Agreement for the Common Access Card. Any Common Access Card-enabled Real-time Automated Personnel Identification System site shall, on presentation of the required documentation, sponsorship, or verification through Defense Enrollment Eligibility Reporting System, issue a Common Access Card to any eligible recipient. Initial issue and renewal of a Common Access Card for contractor employees requires coordination of the sponsoring service contracting official with the intended issuing facility through Trusted Associate Sponsorship System (formerly Contractor Verification System). **Note:** As of November 10, 2005 and October 29, 2010, USD (P&R) Memorandums, *DEERS/RAPIDS Lock Down for Contractors* and *DEERS/RAPIDS Lock Down for Additional Populations*. Defense Enrollment Eligibility Reporting System is locked-down Department wide, requiring all Defense Enrollment Eligibility Reporting System submissions to be made electronically via an authorized data source feed, e.g., Trusted Associate Sponsorship System, formerly the Contractor Verification System, or Military and Civilian Personnel Data Systems to include a positive result from Federal Bureau of Investigation fingerprint check, and an initiated National Agency Check with Inquiries or equivalent.

1.15.1. Any Common Access Card recipient arriving to receive a new credential at a Real-time Automated Personnel Identification System site will not be issued, unless, the applicant's identity, affiliation, a positive result from Federal Bureau of Investigation fingerprint check, and an initiated National Agency Check with Inquiries or equivalent.
1.15.2. The DD Form 577 is the signature card or a signature memorandum which allows the Contracting Officer or government official to sign the DD Form 1172-2 for issuance of the Common Access Card. See DD Form 577 or sample signature memorandum at Attachment 5. **Note**: The Trusted Associate Sponsorship System (formerly, Contractor Verification System), the DD Form 577, signature memorandums, or DD Form 1172-2 will no longer be required for contractor personnel Defense Enrollment Eligibility Reporting System enrollment, with the limited exception of Foreign military and National personnel.
1.15.3. Department of Defense 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.

1.16. Temporary Common Access Card. If a member has been mobilized and there are no communications either with the Defense Enrollment Eligibility Reporting System 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 Public Key Infrastructure certificates and will be replaced as soon as the member can reach an online Real-time Automated Personnel Identification System station or communications have been restored. **Note:** The temporary card will not have an Integrate Circuit Chip, nor will it have Public Key Infrastructure certificates. 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.

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

1.18. Copying Or Distribution Of Cards.
1.18.1. Section 701 of Title 18, United States Code prohibits photocopying or other reproduction of Department of Defense identification cards except by regulation. When possible, the card will be electronically authenticated in lieu of photographing the card. **Note:** The cardholder may allow photocopying of their identification card to facilitate Department of Defense benefits, e.g., processing medical claims.
1.18.2. There are instances where graphical representations of Common Access Cards are necessary to facilitate the Department of Defense mission. When used or distributed, these graphical representations must not be the same size as the Common Access Card and must have the word "SAMPLE" written on them. **Note:** Sample identification cards, not the actual size, with the word 'EXAMPLE" or "SAMPLE" printed across the card may be posted on a Public Key Infrastructure enabled web sites, however, they shall not be posted on public web.

1.19. Restrictions. The Common Access Card shall not be amended, modified, or overprinted by any means. No stickers or other adhesive materials are to be placed on either side of the

Common Access Card. Holes shall not be punched into the Common Access Card, except as required by paragraph 1.5.2. The chip or laminate shall not be removed from the Common Access Card, including rubbing, scratching, or marking out any area on either side of the card. **(T-0).**

1.20. Color Coding. The Common Access Card shall be color coded as indicated below to reflect the status of the cardholder (see Table 1.6).

T**able 1.6. Cardholder Color Coding Status.**

No Color Stripe **"W" White**	U.S. military and Department of Defense civilian personnel or any personnel eligible for a Geneva Conventions card
Blue Color Stripe **(formerly red stripe)** **"B" Blue**	Non-U.S. personnel, including Department of Defense contract employees (other than those persons requiring a Geneva Conventions card)
Green Color Stripe **"G" Green**	All personnel under contract to the Department (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 D/R platform.	

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

1.20.2. Federal Information Processing Standards - 201-1 reserves the red color stripe to distinguish emergency first responder officials.

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

1.22. Roles and Responsibilities. Uniformed Services Defense Enrollment Eligibility Reporting System Project Offices and Real-time Automated Personnel Identification System issuing sites roles will implement Defense Enrollment Eligibility Reporting System enrollment and eligibility policy guidance and procedures relating to identification card eligibility and

issuance, including benefit entitlement eligibility impacting Defense Enrollment Eligibility Reporting System populations.

1.22.1. Uniformed Services Defense Enrollment Eligibility Reporting System Project Offices responsibilities include implementing guidance and procedures to support Real-time Automated Personnel Identification System issuing site tasks. Refer to AFI 36-3026, Volume 1, paragraph 1.5, Verifying Official Responsibilities and Chapter 10 Real-time Automated Personnel Identification System and Defense Enrollment Eligibility Reporting System Procedures.

Chapter 2

PERSONNEL ELIGIBLE FOR THE COMMON ACCESS CARD

2.1. Active, Selected Reserve, and National Guard. The Department of Defense provides Common Access Cards to members of the Department of Defense and military components, Department of Defense contractors including members and contractor populations of the National Oceanic and Atmospheric Administration and the United States Public Health Service, and U.S. Coast Guard, non-Department of Defense Federal civilians, state employees, and other non-Department of Defense affiliates. The Common Access Card 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. 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 Common Access Card.

2.1.1. Members of the National Oceanic and Atmospheric Administration and the United States Public Health Service Common Access Cards shall reflect Uniformed Services.

2.1.2. Reservists on active duty or National Guard members on full-time National Guard duty for 31 days or more will update information on the chip to reflect current military status.

2.2. Foreign Affiliate. Foreign Affiliate (formerly foreign military) personnel qualify for issuance of the United States Department of Defense/Uniformed Services Identification and Privilege Card when the following criteria are met. Foreign personnel will have the U.S. equivalent rank as determined by the sponsoring agency, printed on the Common Access 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 Common Access Card. The Common Access Card will reflect the equivalent rank according to the D/R application. The Department of Defense/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.

2.2.1. Sponsored North Atlantic Treaty Organization and Partnership For Peace in the United States. Active Duty officer and enlisted personnel of North Atlantic Treaty Organization and Partnership For Peace countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Service. A list of North Atlantic Treaty Organization and Partnership For Peace countries can be found in Definitions or http://www.nato.int/pfp/sig-cntr.htm.

2.2.2. Sponsored Non-North Atlantic Treaty Organization Personnel in the United States. Active Duty officer and enlisted personnel of non-North Atlantic Treaty Organization countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Service.

2.2.3. North Atlantic Treaty Organization and Non-North Atlantic Treaty Organization Personnel Outside the United States. Active Duty officer and enlisted personnel of North Atlantic Treaty Organization and non-North Atlantic Treaty Organization countries when serving outside the United States and outside their own country under the sponsorship or

invitation of the Department of Defense or a Military Service, 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 U.S. military establishment.

2.2.4. Non-sponsor North Atlantic Treaty Organization in the United States. Active Duty officer and enlisted personnel of North Atlantic Treaty Organization countries who, in connection with official North Atlantic Treaty Organization duties, are stationed in the United States but are not under Department of Defense or Service sponsorship, and their accompanying dependents living in the non-sponsored North Atlantic Treaty Organization personnel's U.S. household are eligible for benefits. See AFI 36-3026, Volume 1, Attachment 2.

2.3. Civilian Affiliate. Common Access Card eligibility for Department of Defense contractors, non-Department of Defense Federal civilians, State employees, and other non-Department of Defense affiliates is based on the government sponsor's determination of the type and frequency of access required to Department of Defense facilities or networks that will effectively support the mission. Civilian Affiliate, e.g., Inter-governmental Personnel Act.

2.4. Department of Defense/Uniform Services Employees. Department of Defense civilian employees are eligible for one of three Common Access Card 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 AFI 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 Common Access Card.

2.4.1. The United States Department of Defense/Uniformed Services identification Card is issued to Department of Defense civilian employees including National Oceanic and Atmospheric Administration, United States Public Health Service, U.S. Coast Guard 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 Common Access Card issuance.

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

2.4.1.1.4. Non-U.S. citizens employed by or under the sponsorship of Department of Defense.

2.4.1.2. Civilian employees who operate Real-time Automated Personnel Identification System workstations at Federal Agencies, other than Department of Defense (e.g., National

Oceanic and Atmospheric Administration, United States Public Health Service, U.S. Coast Guard).

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

2.4.1.4. State employees of the National Guard.

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

2.4.2. The United States Department of Defense/Uniformed Services Identification and Privilege Card is issued to Common Access Card - 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 Department of Defense 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 Common Access Card identification and Privilege card.

2.4.2.4. Department of Defense 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.

2.4.2.5. Civilian employees of the Air Force Exchange System, Navy Exchange System, Marine Corps Exchange System, and Coast Guard Exchange. 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 Department of Defense/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces is issued to Common Access Card eligible civilian employees who are:

2.4.3.1. Emergency-Essential employees. Emergency-Essential employees as defined in Department of Defense Directive 1404.10 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 Common Access Card 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 Trusted Associate Sponsorship System, formerly, Contractor Verification System to Defense Enrollment Eligibility Reporting System must occur before a Common Access Card can be issued from Real-time Automated Personnel Identification System refer to paragraph 2.5. Refer to Department of Defense Contractor Personnel Office for contractors employed in Germany and Italy.

2.5.1. The United States Department of Defense/Uniformed Services identification Card – the identity credential is issued to eligible contractor employees who are under the terms and conditions of a Department of Defense, Uniformed Services, National Oceanic and Atmospheric Administration, and Public Health Service contract. Contractor employees are required to have physical access to buildings, facilities, installations, and controlled spaces, or access to Department of Defense 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 Common Access Card.

2.5.2. The United States Department of Defense/Uniformed Services identification and Privilege Card – the 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 Common Access Card 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 Department of Defense 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 Common Access Card only, and are not eligible for issuance of the Common Access Card 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 Department of Defense are ineligible for the Common Access Card, example, Department of Energy contractor employee. **Note:** Other Government agency contractors permanently assigned overseas refer to AFI 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 Department of Defense/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces is issued to Common Access Card eligible contractor employees who are: Refer to AFI 36-3026 IP, 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 2 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. 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 Common Access Card.

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 Common Access Card issuance at a Real-time Automated Personnel Identification System facility.

Note: There are separations of duties and responsibilities in the Common Access Card 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 Defense Enrollment Eligibility Reporting System. **(T-0).**

2.7.1. The initial registration process may be performed by the Trusted Associate Sponsorship System, formerly, Contractor Verification System. Military and Civilian Personnel Data Systems provide authoritative data feed to Defense Enrollment Eligibility Reporting System; however, the registration of new members and their identity source document and background investigations shall be followed upon to authenticate a claimed identity prior to Defense Enrollment Eligibility Reporting System enrollment and Common Access Card issuance.

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

2.7.3. The identity source documents must come from a the list of acceptable documents included in U.S. 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.

2.7.3.1. The Verifying Official shall visually inspect the identification documents and verify the document as being genuine and unaltered.

2.8. Central Issuing Facility. Supports the Common Access Card Central Issuance Requesting Station at high-volume Real-time Automated Personnel Identification System military academies and training centers. **Note:** The Central Issuing Facility location is off-site from the Common Access Card Central Issuance Requesting Station and supports the following:

2.8.1. Production of a fully functional and personalized Common Access Card with option to inject:

2.8.1.1. All Public Key Infrastructure and Personal Identity Verification certificates,

2.8.1.2. Identity certificate only, or

2.8.1.3. No Public Key Infrastructure certificates (chip-less)

2.8.2. Mass issuance of Common Access Cards to all uniformed Services cadets/recruits/trainees: active, guard, and reserve members; reduces Real-time Automated Personnel Identification System 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 Common Access Card eligible populations.

2.9. Common Access Card Central Issuance Requesting Station. Defense Manpower Data Center Program Management Review initiative, implemented the Common Access Card Central Issuance Requesting Station at uniformed Services sites with large transient populations, i.e., training centers and Service Academies. Common Access Card Central Issuance Requesting Station converts USID card operations to an enabled Public Key Infrastructure 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 at the Common Access Card Central Issuance Requesting Station 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. **Note:** Batch shipments not received/acknowledge by the Person in Charge or Site Security Manager, 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 Site Security Manager or Person in Charge with alternate back-up personnel are required to secure separate shipments of Common Access Cards and Personal Identification Numbers. The Person in Charge/Site Security Manager will:

2.10.2. Monitor and acknowledge the shipment activity for Common Access Card and Personal Identification Number receipts through the web based Inventory Logistics Portal. Refer to the Inventory Logistics Portal User Guide for card stock and consumable information.

2.10.3. Comply with Public Key Infrastructure/Local Registration Authority Verifying Official Certification Practice Statement responsibilities.

Chapter 3

QUALIFYING REQUIREMENTS AND RESPONSIBILITIES FOR COMMON ACCESS CARD ISSUANCE

3.1. Qualifying Requirements. D/R operators, a minimum of two Site Security Managers and a minimum of one Super Verifying Official. The Site Security Manager and Super Verifying Official can be the same person performing both roles, including the role of Verifying/Issuing Official, Local Registration Authority. The Super Verifying Official also has the ability to access Real-time Automated Personnel Identification System Reports from the COGNOS web application. D/R operators must be U.S. citizens in order to issue Public Key Infrastructure certificates in accordance with Department of Defense 8500.2R, *"Information Assurance (IA),"* 6 February 2003. **(T-0). Note:** Local National and Military Affiliate (foreign national / civilian or military) are not authorized to operate Real-time Automated Personnel Identification System in accordance with the Real-time Automated Personnel Identification System Security Standard Operating Procedure 7.1. In addition, Real-time Automated Personnel Identification System operators are prohibited from becoming a Trusted Agent Security Manager or Trusted Agent for the Trusted Associate Sponsorship System, formerly, Contractor Verification System. Likewise, a Trusted Agent Security Manager and Trusted Agent are not authorized to become a Real-time Automated Personnel Identification System operator as a Site Security Manager or Verifying Official.

3.1.1. Local commanders, agency department head, or their authorized designee shall assign individuals to serve as Site Security Manager, Super Verifying Official, Verifying Official/ Issuing Official /Local Registration Authority following the Grade Authorization for Common Access Card Issuing/Verifying Official/Local Registration Authorization Officials in Attachment 1, Definitions, Issuing/Verifying Official/Local Registration Authority Official. **(T-3).** Access to Real-time Automated Personnel Identification System, (e.g., workstation, deployable, shipboard, and Central Issuing Facility) are restricted to users who are in compliance with the security requirements outlined in the Department of Defense Personnel Security Regulation, Department of Defense 5200.2R and x.509 Certificate Policy for the United States Department of Defense. **Note:** All Real-time Automated Personnel Identification System users are considered Certificate Management Authorities. See Department of Defense 5200.2R Information Technology (IT-II) position category and related duties.

3.1.2. Security Requirements. Military members, Department of Defense Civilian employees and contractor personnel must all meet the security requirements as indicated below. Personnel must:

3.1.3. Have an IT-II security investigation per Department of Defense 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:** Site Security Manager 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).

3.1.3.1. Be a U.S. citizens who serve in the U.S. military, employed as Department of Defense civilians, or are employed as a Department of Defense contractor require a

National Agency Check with Inquiries or equivalent which includes the Federal Bureau of Investigation 10-fingerprint check.

3.1.3.2. Have never been relieved of Certification Authority, Registration Authority, Local Registration Authority, Defense Enrollment Eligibility Reporting System roles or Communication Security custodian duties for reasons of negligence or non-performance of duties.

3.1.3.3. Have never been denied a security clearance, or had a security clearance revoked.

3.1.3.4. Have never been convicted of a felony offense.

3.2. Security Vetting Procedures.

3.2.1. The Site Security Manager will verify that proper background vetting has been completed before logon access will be granted to the Verifying Official, Issuing Official or Local Registration Authority.

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 Site Security Manager by the DMDC/PIPS.

3.3. Training Requirements. All personnel receiving access to D/R will require training and certification through the Defense Manpower Data Center Learning Management System. **(T-0).** Additional information can be found at the following website at https://learning5.dmdc.osd.mil.

3.3.1. The Verifying Official/Local Registration Authority shall be trained on the secure operations of Real-time Automated Personnel Identification System to include printing and encoding a Common Access Card and maintenance of equipment. Defense Manpower Data Center Access Card Office provides web-based training for all Real-time Automated Personnel Identification System users. Site Security Managers, Super Verifying Officials, Verifying Officials, and Issuing Officials 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 Site Security Manager, Super Verifying Official, Verifying Official, and Issuing Official qualifications.

3.3.1.2. Verifies that Real-time Automated Personnel Identification System 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 Real-time Automated Personnel Identification System 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)* is required upon issuance of Common Access Card to a Verifying Official/Issuing Official /Local Registration Authority as part of training. All signed DD Forms 2841 shall be kept locally for training certification. **Note*:*** Site Security Managers trains newly assigned Real-time Automated Personnel Identification System users and provide recurrent training. Training ensures Real-time Automated Personnel Identification System users understand their roles, security procedures, and the implications of performing these procedures correctly. Refer to the Real-time Automated Personnel Identification System Verifying Official Information System web at https://www.dmdc.osd.mil/appj/vois/index.jsp for additional training support materials.

3.4. Verifying Official/Issuing Official And Local Registration Authority. The Verifying Official/Issuing Official/Local Registration Authority responsibilities are to:

3.4.1. Retrieve, limited update, transmits, and store data on the Common Access Card eligible recipients in the Defense Enrollment Eligibility Reporting System 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 Defense Enrollment Eligibility Reporting System, if necessary.

3.4.3. Notify the respective Service Project Office or Defense Manpower Data Center Helpdesk when an invalid entry, lock or unlock of a record in Defense Enrollment Eligibility Reporting System is necessary.

3.4.4. Perform the role of the Local Registration Authority as related to the Public Key Infrastructure functions. Many of the functions are performed automatically through Real-time Automated Personnel Identification System.

3.4.5. Provide and explain to the Common Access Card recipient that their signature on the DD Form 2842, *Subscriber Certificate Acceptance and Acknowledgement of Responsibilities,* acknowledges reading and accepting their responsibilities and obligations as stated.

3.4.6. Perform Common Access Card related processes as further described in Real-time Automated Personnel Identification System User Guide.

3.5. Super Verifying Official. The Super Verifying Official also qualifies as a Verifying Official/Local Registration Authority. In addition, the Super Verifying Official 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.

3.5.1. Generate and examine reports at least once a week, and more often as needed, to identify performance trends, to evaluate Verifying Official 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 disk 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 Verifying Official/Local Registration Authority, Super Verifying Officials and Site Security Manager on Real-time Automated Personnel Identification System using the Certification Practice Statement; Real-time Automated Personnel Identification System User Guide; and the web via Verifying Officer Information System.

3.6. Site Security Manager. The Site Security Manager also qualifies as an Super Verifying Official and Verifying Official/Local Registration Authority. The Site Security Manager must verify the new Verifying Official/Issuing Official/Local Registration Authority is a United States citizen and has satisfied the background vetting requirement. The new Verifying Official/ Issuing Official/Local Registration Authority should be issued a Common Access Card if not already in possession of one with simultaneous completion of the DD Form 2841, *Department of Defense (DoD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities (Registration Official).* The identity certificate is used to authenticate the new Real-time Automated Personnel Identification System Verifying Official. Each site must have

two Site Security Manager and cannot operate without at least one Site Security Manager physically available to attend to all Site Security Manager duties and responsibilities. The Site Security Manager responsibilities are collectively reflected in the Certification Practice Statement, Real-time Automated Personnel Identification System User Guide and as indicated below:

3.6.1. The Site Security Managers are the Real-time Automated Personnel Identification System user administrators for the site and are responsible for and have the authority to activate Real-time Automated Personnel Identification System users and assign or change authorized roles for Verifying Officials, identifications, and Super Verifying Officials. Each Site Security Manager must know the Real-time Automated Personnel Identification System application, rules and procedures. The Defense Manpower Data Center Security Web User Administration tool allows each Site Security Manager to request Defense Enrollment Eligibility Reporting System logon identification, update security privileges for current authorized users. The Site Security Manager ensures password and Personal Identification Numbers remain current, and terminate user access of individuals no longer associated with the issuing site. Each Site Security Manager must ensure that the Verifying Official, Issuing Official, and Super Verifying Official Common Access Cards are updated with Local Registration Authority privileges. Initial training of new users and subsequent training to ensure efficient and secure operations is required.

3.6.2. The Site Security Managers are responsible for the management of Common Access Card stock and related consumables. Common Access Card 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 Site Security Manager is responsible for management of site policies and procedures to ensure the continuous operation of the site and seamless transition of Site Security Managers. These policies include all security policies detailed in the references stated in paragraph 3.2.

3.6.3.1. Each Site Security Manager must also be aware of the various procedures for maintaining a secure and productive site. Key procedures are:

3.6.3.1.1. Arrange for an overlap period between the out-processing and in-processing Site Security Manager.

3.6.3.1.2. Ensure the in-processing Site Security Manager has a Common Access Card with Local Registration Authority privileges, and Real-time Automated Personnel Identification System access. **Note**: Site Security Manager database access for Real-time Automated Personnel Identification System can take as long as 48 hours to be effective.

3.6.3.1.3. A Verifying Official can issue a Common Access Card to the new Site Security Manager, but only an Site Security Manager can request Local Registration Authority privileges for Real-time Automated Personnel Identification System users.

3.6.3.1.4. Ensure Common Access Card issuing equipment is maintained in accordance with the Real-time Automated Personnel Identification System User Guide and guidance from Defense Manpower Data Center in accordance with the Real-time Automated Personnel Identification System Security Checklist and maintains a copy on file. Refer to Real-time Automated Personnel Identification System 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 Real-time Automated Personnel Identification System sites. Long-term failure (4-days or more), contact the Service Defense Enrollment Eligibility Reporting System 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. Defense Enrollment Eligibility Reporting System 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 Real-time Automated Personnel Identification System. Additionally, with the Inventory Logistics Portal system, the Common Access Card stock and supplies shall be delivered only to the site address stored in Defense Enrollment Eligibility Reporting System. For this reason it is critical to maintain current site addresses, email address, and telephone numbers by using the Defense Manpower Data Center 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 Common Access Card stock and supply deliveries.

3.6.4.2. Additional Site Security Manager site administration responsibilities include but are not limited to:

3.6.4.3. Complying with direction from the Defense Manpower Data Center Support Center for viewing or updating Real-time Automated Personnel Identification System Configuration Utilities.

3.6.4.4. Notifying the respective Service Project Office, Defense Manpower Data Center Support Office or agency point of contact when an invalid entry or lock to a record in Defense Enrollment Eligibility Reporting System 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 Site Security Manager 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 Real-time Automated Personnel Identification System software and server-related settings. These tasks include:

3.6.4.5.2. Ensure training of new Verifying Official/Issuing Official /Local Registration Authority s, Super Verifying Officials, and Site Security Managers on the Real-time Automated Personnel Identification System web based training module, Learning Management System.

3.6.4.5.3. Training Verifying Official/Issuing Official/Local Registration Authority, Super Verifying Official, and Site Security Managers on security policies using the Real-time Automated Personnel Identification System Security Standard Operating Procedure (see Definitions).

Chapter 4

REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM SITE MANAGEMENT

4.1. Cardstock Management. Site Security Manager must use the Inventory Logistics Portal to manage the Common Access Card 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 Site Security Manager's Common Access Card for access.

4.1.2. The Inventory Logistics Portal will be used to replenish all Common Access Card cardstock and related consumables. Inventory Logistics Portal automatically generates orders based on Common Access Card 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 Site Security Managers at the site's address location registered in Defense Enrollment Eligibility Reporting System.

4.1.2.1. If a Common Access Card 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 Common Access Card cardstock using the order form from the Verifying Official Information System web site https://www.dmdc.osd.mil/appj/vois/index.jsp.

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

4.2. Card Handling and Storage Guidelines. Sites are responsible for safeguarding their Common Access Card cardstock and equipment in a secure location. **(T-3).** (Refer to the Real-time Automated Personnel Identification System Verifying Official 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 Inventory Logistics Portal which manages the levels of inventory at each Real-time Automated Personnel Identification System site. When the Inventory Logistics Portal is not available, order Common Access Card consumables using the order form https://www.dmdc.osd.mil/appj/vois/index.jsp. The Defense Manpower Data Center /Personnel Identity Protection will provide Real-time Automated Personnel Identification System sites with consumables based on their Common Access Card production volume, including color printer ribbons and laminate rolls. Additional consumable replacements are processed through the appropriate SPO to Defense Manpower Data Center. Refer to the Real-time Automated Personnel Identification System 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 Site Security Manager 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 Real-time Automated Personnel Identification System 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, February 2008. All Real-time Automated Personnel Identification System 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 Real-time Automated Personnel Identification System 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 Personal Identity Verification 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 Common Access Card is Department of Defense Personal Identity Verification credential used to facilitate physical access to facilities and installations and enable logical access to Department of Defense networks. This guidance does not address procedures or requirements related to the use of the Common Access Card for physical access to facilities or installations or for access to Department of Defense networks. These areas are addressed in separate Department of Defense guidance from USD(I) and ASD(NII).

5.1.2. In addition to the current Common Access Card capabilities, the Common Access Card 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. Public Key Infrastructure 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-Department of Defense Federal Government employees affiliated with the Department) that may still require the issuance of a Common Access Card to support their Department of Defense assignment, benefits entitlements, or Geneva Conventions requirements. To be issued a Common Access Card, these individuals will be required to apply for a waiver to the Common Access Card eligibility policy through the Office of the USD (P&R). Waivers will be reviewed and granted on a case-by-case basis.

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. Common Access Card eligible personnel must be registered in Defense Enrollment Eligibility Reporting System through either an authoritative

personnel data feed from the appropriate Service, Agency, the Trusted Associate Sponsorship System, formerly, Contractor Verification System.

5.4. Initial Issuance – Eligibility, Affiliation, Background Vetting, And Claimed Identity. Identity Verification. During the Common Access Card issuance process, all personnel will present two forms of identification in original form to verify a claimed identity. 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 list shall be a valid (unexpired) State or Federal Government-issued picture identification. The identity documents will be inspected for authenticity and scanned and stored in the Defense Enrollment Eligibility Reporting System according to the Real-time Automated Personnel Identification System User Guide upon issuance of an identification. 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 Common Access Card 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. The card issuer will verify the cardholder's identity against the biometric information stored in Defense Enrollment Eligibility Reporting System. Consistent with applicable law, the applicant shall be required to provide identity source documents.

5.5.2. The Common Access Card is reported lost or stolen. The card issuer will verify the cardholder's identity against the biometric information stored in Defense Enrollment Eligibility Reporting System and confirm the expiration date of the missing Common Access Card. The individual shall be required to present documentation from the local security office or Common Access Card sponsor confirming that the Common Access Card has been reported lost or stolen. This documentation must be scanned and stored in Defense Enrollment Eligibility Reporting System. The individual reporting a lost, stolen, or destroyed ID shall be required to provide identity source documents as noted on Attachments 4, 10, and 11. The replacement Common Access Card will have the same expiration date as the lost or stolen card.

5.6. Expiration Dates. Local commands, installations, and sponsors of contract support personnel and other eligible Common Access Card holders will establish procedures to ensure that the issuance and retrieval of Common Access Cards are part of the normal personnel check-in and check-out processes. These procedures will identify who will have responsibility to retrieve Common Access Cards 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 Common Access Cards will be documented and treated as personally identifiable information or identification of a person, according to Department of Defense Directives 5400.11 and 5200.01 and returned to a Real-time Automated Personnel Identification System site for disposition.

5.6.1. Invalid, inaccurate, inoperative, terminated, or expired Common Access Cards shall be returned to a Real-time Automated Personnel Identification System site for disposition. The Common Access Card is the property of the U.S. Government and shall not be retained by the

cardholder upon expiration, replacement, or when the Department of Defense affiliation of the employee has been terminated. **Note:** Common Access Card is issued with a three-year expiration date. **Exception**: Services academies - Common Access Cards are issue with a 4-year expiration date with a three-year Public Key Infrastructure certificate.

5.7. Common Access Card Public Key Infrastructure Certificates. Using Real-time Automated Personnel Identification System, the identity certificate will be issued on the Common Access Card at the time of card issuance in compliance with the X.509 *Certificate Policy for the United States Department of Defense.* E-mail signature and e-mail encryption certificates may also be available on the Common Access Card either upon issuance or at a later time, including the availability of the Personal Identity Verification Authentication. If the person receiving a Common Access Card does not have an organization e-mail address assigned to them, they may return to a Real-time Automated Personnel Identification System 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 Common Access Card, 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 Department of Defense who have multiple Defense Enrollment Eligibility Reporting System Personnel Category Code 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. Multiple current identification cards will not be issued or exist for an individual under a single Personnel Category Code in Defense Enrollment Eligibility Reporting System. **(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 Defense Enrollment Eligibility Reporting System 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 Real-time Automated Personnel Identification System station or communications have been restored.

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 or body piercing accruements, etc. **(T-0).** The following provides general guidance concerning photographs for the Common Access Card:

5.10.1. Individual will poise with a frontal, full-face (passport-type) photo shot. Individual's composure will reflect similar to guidelines posted by the U.S. Department of State for passport issuance listed at www.travel.state.gov/passport. 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 members must comply with their respective Service grooming standards. **Note:** Active, Selected Reserve, Participating Individual Ready Reserve, and Volunteer Training Unit members must also be within Service dress and appearance standards when in civilian attire. This also applies to members who are on appellate leave. Refer to AFI 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 AFI 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.

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, U. S. 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**,** Navy Personnel Command (PERS-24), 5720 Integrity Drive, Millington, Tennessee 38055-6730, (901) 874-4862. Fax (901) 874-2766.

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 - DEPARTMENT OF THE AIR FORCE, HQ AFPC/DP3SA, 550 C Street West, JBSA Randolph Texas 78150-4739, (210) 565-2089 or Defense Switch Network 665-2089; Fax: Defense Switch Network 665-6224 or (210) 565-6244; E-mail: afpc.dp2ssm.deers@us.af.mil.

6.1.6. AIR FORCE RESERVE/AIR NATIONAL GUARD– HQ AIR RESERVE PERSONNEL CENTER, 18420 East Silver Creek Ave Bldg 390, MS68, Buckley AFB, Colorado 80011, (720) 847-3886 or Defense Switch Network 847-3886; Fax (720) 8473886, 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, U.S. 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, U.S. 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, U.S. Coast Guard, Personnel Service Center (PSC), U.S. 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), U.S. 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/RETIRED UNITED STATES PUBLIC HEALTH SERVICE* - UNITED STATES PUBLIC HEALTH SERVICE, Division of Commissioned Corp Personnel Readiness, DCCPR, 1101 Wootton Parkway, Plaza Level, Suite 100, Rockville, Maryland 20852, (240) 453-6131. Fax: (240) 453-6134, E-mail phsdeersgibill@hhs.gov.

6.1.15. *FEDERAL AGENCIES CVS or ENROLLMENTS* – Trusted Associate Sponsorship System (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) U.S. 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.

DANIEL R. SITTERLY
Acting Assistant Secretary of the AF
(Manpower and Reserve Affairs)

GERALD B. O'KEEFE
Deputy Administrative Assistant to the Secretary of the Army/Executive Director, Resources Program Agency

KENNETH R. WHITESELL, USN
Commander, Navy Personnel Command

R. E. MILSTEAD, Lt General, USMC
Deputy Commandant for
Manpower and Reserve Affairs

STEVEN E. DAY, RADM, USCG
Acting Director of Reserve and Military Personnel

MICHAEL S. DEVANY, RADM
Director, National Oceanic and Atmospheric Administration Corps

JOAN F. HUNTER, RADM, USPHS
Director, Division of Commissioned Corps Personnel Readiness

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons, 22* November 1943

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 10, United States Code, Section 1074, Medical and Dental Care for Members and Certain Former Members

Title 10, United States Code, Section 1076(a) and 1086(c)(2), TRICARE Dental Program and Contracts for Health Benefits for Certain Members, Former Members and their Dependents

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

Title 10, United States Code, Section 8013, Secretary of the Air Force

Title 10, United States Code, Section 3013, Secretary of the Army

Title 10, United States Code, Section 5013, Secretary of the Navy

Public Law 102-484, National Defense Authorization Act, 23 October 1992

Public Law 107-107, National Defense Authorization Act, 28 December 2001

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

Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS 201-1), August 2013

DoD Instructions 1000.1, *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,* January 23, 2014

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

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

Directive-Type Memorandum (DTM) 08-006, *Next Generation Common Access Card Implementation Guidance,* Incorporating Change 4, October 4, 2012

Directive-Type Memorandum (DTM) 08-003, *Next Generation Common Access Card Implementation Guidance,* Incorporating Change 5, October 8, 2013
Directive-Type Memorandum 12-004, *DoD Internal Information Collections,* 24 April 2012

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

DoD Instruction 1341.2, *Defense Enrollment Eligibility Reporting System Procedures,* 19 March 1999

DoD Instruction 1015.10, *Military Morale, Welfare, and Recreation (MWR) Programs,* 6 July 2009

DoD Instruction 1330.17, *Armed Services Commissary Operations,* 18 June 2014

DoD Instruction 1330.21, *Armed Services Exchange Regulations*, 14 July 2005

DoD Directive 5000.02, *The Defense Acquisition System,* 12 May 2003

DoD Directive 8500.01, *Information Assurance (IA),* 24 October 2002

DoD Directive 5230.20, *Visits and Assignments of Foreign Nationals,* 22 June 2005

DoD Directive 5400.11, *DoD Privacy Program,* October 29, 2014

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

DoD Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information,* February 24, 2012, Incorporating Change 2, March 19, 2013

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

DoD Regulation 5200.02, *Personnel Security Program,* 21 March 2014

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

DoDI 8910.1M, *Department of Defense Instruction for Information Collection and Reporting,* 19 May 2014

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

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,* August 5, 2005

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,* August 5, 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

DoD Directive 1404.10, *DoD Civilian Expeditionary Workforce,* 23 January 2009

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

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

Assistant Secretary of Defense for Health Affairs Memorandum, *Medical Care Costs for*

Civilian Employees Deployed in Support of Contingency Operations, 8 January 1997

Chapter 15, Sections 331-335, 688, 1581, 1588, 12301(a), 12032, 12304, 12305, and 12406 of

AFPD 36-30, *Military Entitlements,* 28 April 2015

AFI 31-101, *Integrated Defense,* 8 October 2009

AFI 33-360, *Publications and Forms Management,* 1 December 2015

AFI 36-3026, IP, Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel, (new publication date pending)*

AFMAN 33-223, *Communication and Information, Identification and Authentication, 29* July 2005

AFI 33-363, *Communication and Information, 18* May 2006

Prescribed Forms

None

Adopted Forms

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

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*

DD Form 2ACT, *Armed Forces of the United States Geneva Conventions Identification Card (Active) (Green)*

DD Form 2RES, *Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)*

DD Form 2RET, *United States Uniformed Services Identification Card (Retired) (Blue)*

DD Form 1173S, *United States Uniformed Services Identification and Privilege Card (Tan)*

DD Form 1173-1, *United States Uniformed Services Identification and Privilege Card (Red)*

DD Form 1934, *Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces*

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

DD Form 2764**,** *United States DoD/Uniformed Services Civilian Geneva Conventions Card (Storage Safeguard)*

DD Form 2765, *Department of Defense/Uniformed Services Identification and Privilege Card (Storage Safeguard)*

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*

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

CoN - Certificate of Networthiness

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

PIP - Personnel Identity Protection

RA - Registration Authority

RAPIDS - Real Time Automated Personnel Identification System

SPO - Service Project Office

SSA - Social Security Administration

UMP/PIP – User Maintenance Portal/Post Issuance Portal

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 tele-work, Virtual Private Network, and remote administration by Department of Defense or non-DoD personnel, (including U.S. Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service).

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/Department of Defense employee. When individual is not a Real-time Automated Personnel Identification System Verifying Official/Local Registration Authority, the Authorizing/Verifying Official 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 Personal Identity Verification credentialing.

Certificate of Networthiness (CoN) - 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 Department of Defense Public Key Infrastructure 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 Department of Defense 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 Verifying Officials/Local Registration Authorities (Verifying Officials/Local Registration Authority) meet the requirements set forth in the CP policy.

Certificate Management Authority - A Certification Authority or 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 Common Access Card.

Civilian employee - Department of Defense 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 U.S. Coast Guard, National Oceanic and Atmospheric Administration , and Public Health Service). 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 Department of Defense 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 Personal Identity Verification Authentication. The Personal Identity Verification certificate enables the Common Access Card to be Homeland Security Presidential Directive-12 compliant and interoperable with other Federal Agencies and their Public Key Infrastructures. August 24, 2014, the Common Access Card is issued with the Personal Identity Verification 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 - means 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 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 U.S. citizens, U.S. legal aliens, third country national personnel, and citizens of host nations, who are authorized to accompany U.S. military forces in contingency operations, other military operations, or exercises designated by the geographic combatant commander (including U.S. Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service). 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 Department of Defense, 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 U.S. Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service). For the purposes of Common Access Card issuance and expiration dates on the Common Access Card, 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 Common Access Card that expires in a maximum of 3 years so long as the Common Access Card can be revoked upon termination of the contract)

Defense Enrollment Eligibility Reporting System - A computer-based enrollment and eligibility system that the Department of Defense 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. Defense Enrollment Eligibility Reporting System can interact with and support systems such as the Real-time Automated Personnel Identification System and other programs within Department of Defense and the military departments.

Dependent - An individual whose relationship to the sponsor leads to entitlement to benefits and privileges, and children of same-sex marriage and family members only. See Family Member Term in AFI 36-3026, Volume 1.

Defense Agencies and Offices - All agencies and offices of the Department to Defense, 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 Department of Defense 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 Real-time Automated Personnel Identification System 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. Excepted service positions. 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 AFI 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 Common Access Card eligible if sponsored by their government as part of an official visit or assigned to work on a Department of Defense facility and/or require access to Department of Defense 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 military personnel. - The card will reflect the Equivalent (EQ) rank, example "Major." The Department of Defense/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 North Atlantic Treaty Organization and Partnership For Peace personnel in the United States**. Active** duty officer and enlisted personnel of North Atlantic Treaty Organization and Partnership For Peace countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department. Sponsored non-North Atlantic Treaty Organization personnel in the United States. Active duty officer and enlisted personnel of non-North Atlantic Treaty Organization countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department. North Atlantic Treaty Organization and non-North Atlantic Treaty Organization personnel outside the United States - AD officer and enlisted personnel of North Atlantic Treaty Organization and non-North Atlantic Treaty Organization countries when serving outside the United States and outside their own country under the sponsorship or invitation of the Department of Defense 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 U.S. military establishment. Non-sponsored North Atlantic Treaty Organization personnel in the United States. AD officer and enlisted personnel of North Atlantic Treaty Organization countries who, in connection with their official North Atlantic Treaty Organization duties, are stationed in the United States and are not under the sponsorship of the Department of Defense or a Military Department, are not eligible for a Common Access Card, 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 Common

Access Card or Volunteer Logical Access Credential if the mission requires it. See AFI 36-3026, Volume 1, Issuing/Verifying Official Term.

Government Sponsor – Based on the Department of Defense government sponsor's determination (including U.S. Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service) of the type, and frequency of access required to Department of Defense facilities, or networks that will effectively support the mission.

Homeland Security Presidential Directive-12 - A new 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.

Intermittent work schedule. Employment without a regularly scheduled tour of duty.

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 and 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.

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 Defense Enrollment Eligibility Reporting System enrollment).

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 Department of Defense shall include a credit check.

Non-appropriated funds employees. Federal employees within the Department of Defense 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 Department of Defense.

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, Personal Identity Verification of Federal Employees and Contractors, includes the architecture and technical requirements for a government-wide Personal Identity Verification 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 Personal Identity Verification card is the primary component of the Personal Identity Verification 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, Personal Identity Verification 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 Personal Identity Verification 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 Defense Enrollment Eligibility Reporting System database to provide on-line processing of information to the Defense Enrollment Eligibility Reporting System database.

Real-time Automated Personnel Identification System Self-Service (RSS) Portal - Replaces the existing User Maintenance Portal/Post Issuance Portal (UMP/PIP) functionality used for adding or updating E-mail address and to receive initial or new Public Key E-mail signature and E-Mail encryption certificates, add a Personnel Category Code to the User Principle Name of E-mail certificate, activation of the Personal Identity Verification certificate, and adding the Joint Data Model applet to the Common Access Card.

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 Individual Ready Reserve, and the ING.

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 Common Access Card applicants.

Senior Executive Service positions - Department of Defense 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 – An Active Duty member or civil servant who approves a Common Access Card request.

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

Verifying Official/Local Registration Authority - A person who is a US citizen and authorized by the Chief of Issuing Activity to be a Verifying Official/Local Registration Authority military member, Department of Defense civilian (appropriated or non-appropriated fund—supported), equivalent civilian personnel employed by the National Guard of the United States, or a foreign national responsible for issuing identification cards. For Verifying Officials 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, and the only person authorized to sign block numbers

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 U.S. Army Criminal Investigation Command; Naval Criminal Investigative Service; Air Force Office of Special Investigation; Marine Corps, Naval Criminal Investigative Service; and Coast Guard Intelligence.

Special Agent Offices - US Army Criminal Investigative Command; Naval Criminal Investigative Service; Air Force Office of Special Investigation; Marine Corps, Naval Criminal Investigative Service; and Coast Guard 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.

Tier Definitions -Tiers 0, 1, 2, and 3 applies as approved by the Air Force Inspector General Advisory Board to AD, ANG and AFRC units using Real-time Automated Personnel Identification System in identifying Tier waiver authorities (T-0, T-1, T-2, and T-3).

Tier 0 (T-0) - Determined by respective non-AF authority (e.g. Congress, White House, Office of Secretary of Defense, Joint Staff). The waiver authority is non-applicable, or external to AF.

Tier 1 (T-1) - Non-compliance puts Airmen, Commanders or the USAF strongly at risk of mission or program failure, death, injury, legal jeopardy or unacceptable fraud, waste or abuse. The waiver authority is the Major Command/CC, delegable no lower than Major Command Director, with the concurrence of the AFI Certifying Official.

Tier 2 (T-2) - Non-compliance may degrade mission or program effectiveness or efficiency and has potential to create moderate risk of mission or program failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. The waiver authority is the Major Command/CC (delegable no lower than Major Command Director).

Tier 3 (T-3) - Non-compliance may limit mission or program effectiveness or efficiency and has a relatively remote potential to create risk of mission or program failure, injury, legal jeopardy or unacceptable fraud, waste, or abuse. The waiver authority is the Wing/DRU/FOA/CC (delegable no lower than Group/CC or equivalent).

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

Trusted Agent - Trusted Associate Sponsorship System, formerly the Contractor Verification System, the Trusted Associate Sponsorship System Trusted Agent Security Manager or Trusted Agent must be certified, trained, and a U.S. citizen and a U.S. government employee, U.S. military or U.S. Department of Defense civilian, and possess a valid Common Access Card. The Trusted Associate Sponsorship System/Contractor Verification System Trusted Agent Security Manager/TA duties are separate, by ensuring the *enrollment* authority (via Trusted Associate Sponsorship System web application) and the *issuance* authority (via Real-time Automated Personnel Identification System workstation) are not the same entity (shared duties), IAW Federal Identity Processing Standard 201.

Verifying Official/Local Registration Authority Certification Process – Verifying Official/Local Registration Authority must be certified, trained, and a U.S. 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 Common Access Card recipient has appropriate identification; completing and correctly disposing of the forms involved in the Common Access Card issuance process, and collecting and disposing of any Common Access Card or other identification cards returned.

Voluntary Training Unit - A unit formed by volunteers to provide Reserve Component training in a non-pay status for Individual Ready Reservists 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. The following guidance applies to only those Common Access Cards with which benefits and privileges are associated, consequently the United States Department of Defense/Uniformed Services Identification Card is not included. See AFI 36-3026, Volume 1, Attachment 2 for inclusive listing of benefits and privileges.

Abbreviations:

CHC Civilian Health Care
DC Direct Care at Military Treatment Facility
C Commissary
MWR Morale, Welfare, & Recreation
E Exchange

Table A2.1. Armed Forces of the United States Geneva Conventions Identification Card. The benefits and privileges administered by the Uniformed Services exist primarily to benefit the members of those Services. It is understood that the members automatically are entitled to the benefits and privileges indicated below; consequently their privileges are not printed on the surface of the Common Access Card. The privileges are, however, embedded within the technologies of the Common Access Card, and can be modified, as necessary.

	CHC	DC	C	MWR	E
Active	No	Yes	Yes	Yes	Yes
Reserve	No	No	Yes	Yes	Yes
Guard	No	No	Yes	Yes	Yes
Note: Reserve and National Guard members, on AD for 31 days or more, including their eligible dependents are eligible medical care. See AFI 36-3026, Volume 1, Attachment 2.					

Table A2.2. United States Department of Defense/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces. The benefits and privileges administered by the Uniformed Services are authorized contingent on factors relating to permanent assignment, temporary duty during a conflict, combat, or contingency, either in continental United States or Overseas Continental United States and on availability at the location.

	CHC	DC	C	MWR	E
Continental United States Assigned: Emergency-Essential civilian, contingency contractor, civilian noncombatants authorized to accompany US forces in regions of	No	1&2	1&2	1&2	1&2

conflict, combat and contingency operations liable to capture and detention as Prisoner of War					
Emergency-Essential employee permanently stationed Overseas Continental United States	No	3&4	Yes	Yes	Yes
Contingency Contractor permanently stationed Overseas Continental United States	No	3&5	5	5	5
Overseas Continental United States civilian noncombatants authorized to accompany US forces in regions of conflict, combat and contingency operations liable to capture and detention as Prisoner of War	No	3&4	Yes	Yes	Yes

Notes:
1. The authorized patronage block for eligible individuals permanently assigned in continental United States will be blank. Travel orders authorize access for these individuals while enroute to the deployment site.
2. During a conflict, combat, or contingency operations, civilian employees with this Common Access Card will be granted all commissary, exchange, Morale, Welfare, and Recreation, and medical privileges available at the site of the deployment, regardless of the statements on the identification card.
3. Civilian employees and contractors providing support when forward deployed during a conflict, combat, or contingency operation are treated in accordance with the ASD(HA) memorandum of January 8, 1997, subject: "Medical Care Costs for Civilian Employees Deployed in Support of Contingency Operations."
4. Yes, on a space-available, fully reimbursable basis.
5. Contractor employees possessing this card shall receive the benefit of those commissaries, exchange, Morale, Welfare, and Recreation, and medical privileges that are accorded to such persons by international agreements in force between the United States and the host country concerned.

A2.1.1. The Authorized Patronage block for eligible individuals who are permanently assigned in foreign countries (it should be noted that local nationals are in their home country, not a foreign country) will have the word "OVERSEAS" printed within the block of the Common Access Card.

A2.1.2. The Authorized Patronage block for eligible individuals permanently assigned in continental United States will be blank. Travel orders authorize access for these individuals while enroute to the deployment site.

A2.1.3. During a conflict, combat, or contingency operation, civilian employees with a United States Department of Defense/Uniformed Services Geneva Conventions identification Card for Civilians Accompanying the Armed Forces (Overseas Continental United States location) will be granted all commissary, exchange, Morale, Welfare, and Recreation, and medical privileges available at the site of the deployment, regardless of the statements on the identification card. Contractor employees possessing this identification card shall receive the benefit of those commissaries, exchanges, Morale, Welfare, and Recreation facilities, and

medical privileges that are accorded to such persons by international agreements in force between the United States and the host country concerned.

A2.1.4. The medical block on this card will contain a statement, "When TAD/Temporary Duty or stationed overseas on a space-available fully reimbursable basis." However, civilian employees and contractual services employees providing support when forward deployed during a conflict, combat, or contingency operation are treated in accordance with the ASD(HA) memorandum of January 8, 1997, subject: "Medical Care Costs for Civilian Employees Deployed in Support of Contingency Operations." This policy states that it is not considered practicable or cost-effective to seek reimbursement from civilian or contractor employees or third party payers for medical services. However, where a civilian or contractor employee is evacuated for medical reasons from the contingency area of operations to a Medical Treatment Facility funded by the Defense Health Program, normal reimbursement policies would apply for services rendered by that facility.

Table A2.3. United States Department of Defense/Uniformed Services Identification and Privilege Card. Primary identification card (granting applicable benefits and privileges), and physical and logical access for civilian employees and eligible recipients in the following categories:

	CHC	**DC**	**C**	**MWR**	**E**
Civilian employees of the DoD and the Uniformed Services, when required to reside in a household on a military installation within the Continental United States, Hawaii, and Alaska.	No	No	1	Yes	2
Civilian employees of the DoD, the Uniformed Services, and civilian personnel under private contract to the DoD or a Uniformed Service, when stationed or employed and residing in foreign countries for a period of at least 365 days.	No	3	Yes	Yes	Yes
Civilian personnel of the DoD and the Uniformed Services, and civilian personnel under private contract to the DoD or a Uniformed Service when stationed or employed in Puerto Rico or Guam	No	4	5	Yes	2
Department of Defense Presidential Appointees who have been appointed with the advice and consent of the Senate. (See **Note** 1.)	No	6	No	No	No
Civilian employees of the Army and Air Force Exchange System, Navy Exchange System, and Marine Corps Exchange System, U.S. Coast Guard Exchange System within Continental United States & Overseas	No	No	No	No	7

Military Affiliate (formerly Foreign Military) Personnel:					
1. Sponsored North Atlantic Treaty Organization and Partnership for peace in the United States. AD officer and enlisted personnel of North Atlantic Treaty Organization and Partnership For Peace countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Service.	No	8	Yes	Yes	Yes
	No	9	Yes	Yes	Yes
2. Sponsored Non- North Atlantic Treaty Organization Personnel in the United States. AD officer and enlisted personnel of non-North Atlantic Treaty Organization countries serving in the United States under the sponsorship or invitation of the DoD or a Military Service.	No	9	Yes	Yes	Yes
3. North Atlantic Treaty Organization and Non-North Atlantic Treaty Organization Personnel Outside the United States. AD officer and enlisted personnel of North Atlantic Treaty Organization and non-North Atlantic Treaty Organization countries when serving outside the United States and outside their own country under the sponsorship or invitation of the Department of Defense or a Military Service, 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 U.S. military establishment.	No	8	No	Yes	Yes
4. Non-sponsored North Atlantic Treaty Organization personnel in the United States. AD officer and enlisted personnel of North Atlantic Treaty Organization countries who, in connection with their official North Atlantic Treaty Organization duties, are stationed in the U.S. but are not under Department of Defense or Service sponsorship.					

Notes:
1. Yes, but commissary privileges do not include the purchase of tobacco products in those States including the District of Columbia, that impose a tax on such products.
2. Yes, are entitled to limited exchange privileges, which include purchase of all items except uniform articles and State tax-free items.
3. Yes, on a space-available, fully reimbursable basis.
4. Yes, on a space-available, fully reimbursable basis only if residing in a household on a military installation.
5. Yes, when hired in continental United States under a transportation agreement. **Note:** Puerto Rico and Guam are considered overseas. Therefore, employees hired in the continental United States under a transportation agreement for employment in Puerto Rico and Guam are not required to reside on a military installation to be eligible for commissary privileges.
6. Yes, Presidential Appointees are authorized medical and emergency dental care in military medical and/or dental treatment facilities within 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.
7. Yes, Exchange employees are entitled to all privileges of the exchange system, except for purchase of articles of uniform and state tax-free items.
8. Yes, for outpatient care no charge and for inpatient care at full reimbursable rate.
9. Yes, for outpatient care only on a reimbursable basis.

A.2.1.5. Presidential Appointees are authorized medical and emergency dental care in military medical and/or dental treatment facilities within the Contiguous 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.

A2.1.6. Exchange employees are entitled to all privileges of the exchange system, except for purchase of articles of uniform and state tax-free items.

A2.1.7. Non-sponsored North Atlantic Treaty Organization Personnel in the United States. Active Duty officer and enlisted personnel of North Atlantic Treaty Organization countries who, in connection with their official North Atlantic Treaty Organization duties, are stationed in the United States and are not under the sponsorship of the Department of Defense or a Military Service are not eligible for a Common Access Card, and will continue to receive a DD Form 2765.

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 Defense Enrollment Eligibility Reporting System. In all cases refer to Tables A3.1 and A3.2. **Note:** Under Secretary of Defense, Personnel & Readiness (USD [P&R]) Memorandum, October 29, 2010, *"DEERS/RAPIDS Lock Down for Contractors,"* November 2005, Department of Defense identification card eligible populations shall have their information entered and verified in Defense Enrollment Eligibility Reporting System using a secure automated personnel data feed by the Trusted Associate Sponsorship System, formerly, Contractor Verification System, or as determined by the Defense Manpower Data Center and the sponsoring Service/Agency. Non-U.S. person non-appropriated fund employees shall continue to have their information manually entered at a Real-time Automated Personnel Identification System workstation via DD Form 1172-2.

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. Non-Federal Agency Associate – verified DD Form 1172-2.
Contractor	Contractor (DoD and Uniformed Service) – the Trusted Associate Sponsorship System, formerly, Contractor Verification System enrollment to Defense Enrollment Eligibility Reporting System. Contractor (Other Federal Agency) – verified DD Form 1172-2 or Letter of Authorization
DoD Civilian Employee	Civil Service (DoD and Uniformed Service) – Defense Civilian Personnel Data System enrollment to Defense Enrollment Eligibility Reporting System. 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.
Foreign Affiliate	Foreign military AD member – Invitational travel order or other document reflecting sponsorship by the Department of Defense or uniformed Service, or verified DD Form 1172-2. **Note:** The card will reflect the Equivalent (EQ) rank, example "Major." The Department of Defense/uniformed Service sponsoring agency should 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
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.

Table A3.2. Documentation Required To Determine Type Of Common Access Card For Civilian And Contractor Employees. There are four **Common Access Card** types used within the DoD/Uniformed Services, based on eligibility. Refer to Chapter 1 for each Common Access Card description.

Personnel Status	Common Access Card	Documentation/Information source
Civilian employees	Identification **Common Access Card**	1. Defense Civilian Personnel Data System enrollment to DEERS, or 2. Not in DEERS (civilian retired), verified DD Form 1172-2 as supported by SF Form 50, *Notification of Personnel Action*
	Identification and Privilege Common Access Card (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 Common Access Card 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 Department of Defense 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 Common Access Card	Trusted Associate Sponsorship System, formerly, **Contractor Verification System** enrollment to Defense Enrollment Eligibility Reporting System.
	Identification and Privilege Common Access Card (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 Common Access Card 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 Common Access Card 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.

A3.1.1. Common Access Card eligible individuals requiring enrollment to Defense Enrollment Eligibility Reporting System through a personnel data feed contact the respective Service DEERS/RAPIDS/Public Key Infrastructure Project Office, Department Agency, or the Defense Manpower Data Center Support Office. See Chapter 6, UNIFORMED SERVICES DEERS/RAPIDS PROJECT OFFICES, DMDC SUPPORT CENTER (DSC).

Attachment 4

DEPARTMENT OF HOMELAND SECURITY U.S CITIZENSHIP AND IMMIGRATION SERVICES (USCIS) Form 1-9, "EMPLOYMENT ELIGIBILITY VERIFICATION" AND LISTS OF ACCEPTABLE DOCUMENTS

See Form 1-9 Lists of Acceptable Documents for identity proofing, Defense Enrollment Eligibility Reporting System enrollment, eligibility, and ID card issuance purposes. Eligible individuals are required to provide two forms of IC according to I-9 at http://www.uscis.gov/portal/site/uscis.

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 DD Form 2 (Reserve, Retired, and Reserve Retired), a DD Form 1173, a DD Form 1173-1, a DD Form 2764, a DD Form 2765, and a Common Access Card for eligible individuals who are not enrolled in the Defense Enrollment Eligibility Reporting System or to update eligible individual's Defense Enrollment Eligibility Reporting System record. Retention and disposition of the DD Form 1172-2 shall be in accordance with uniformed services' regulatory instructions.

A5.1.2. DoD sponsors enrolling their dependents in Defense Enrollment Eligibility Reporting System should complete Sections I, II, and IV.

A5.1.3. Department of Defense 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 Common Access Card should complete Sections I and II (and Section IV if a Foreign Affiliate on orders to the U.S. with authorized Dependents). The DD Form 1172-2 should then be provided to a Department of Defense Sponsor for authorization and completion of Section III.

A5.1.5. Department of Defense sponsors authorizing a Common Access Card for an employee should complete Section III.

A5.1.6. For certain populations a paper form will not be required. (Populations entered into Real-time Automated Personnel Identification System via Trusted Associate Sponsorship System (formerly the Contractor Verification System).

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

A5.2. SECTION I. SPONSORS/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. Gender. Enter the sponsor/employee's gender from the valid codes listed in Table 1: (Use one character code M or F).

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

Code	Gender
M	**Male**

F	**Female**

A5.2.3. Block 3. Social Security Number or Department of Defense ID Number.

A5.2.4. Enter the sponsor/employees' Social Security Number or Department of Defense ID Number. In cases where an employee has not been issued an Social Security Number or Department of Defense 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 military 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.

A.5.2.5. For VOs: If a Social Security Number or Department of Defense ID Number is already registered in Defense Enrollment Eligibility Reporting System 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

A5.2.6. Block 4. Status. Enter the sponsor/employee status from the valid codes listed in Table 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 military 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 U.S. 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 AFI 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 3. (Use no more than five characters.)

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

CODE	ORGANIZATION
USA	U.S. Army
USAF	U.S. Air Force
USN	U.S. Navy

USMC	U.S. Marine Corps
USCG	U.S. Coast Guard
USPHS	U.S. Public Health Service
NOAA	National Oceanic and Atmospheric Administration
DoD	Department of Defense
FED	Employee of an Agency other than D Department of Defense
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 4. (Use no more than four characters.)

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

CODE	BRANCH OF SERVICE
El-E9	Enlisted pay grades 1 through 9
W1-W5	Warrant officer 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 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 6. Use two characters.
(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	CR	Macedonia	MK	Thailand	TH

Islands					
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 7. If place of birth is a foreign country, enter the country from the valid codes from Table 6.

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

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

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 U.S. postal code for the State of the sponsor/employee's residence from the valid codes listed in Table 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 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 U.S. postal code for the State of the sponsor/employee's duty location from the valid codes listed in Table 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 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 Defense Enrollment Eligibility Reporting System 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, Real-time Automated Personnel Identification System 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.

A5.3.2.2. When the sponsor is deceased each of the survivors (widow, widower, children, parent, parent in-law, and step-parent) shall sign for themselves. **Note:** When the surviving spouse is a step parent, do not have the step parent 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 Verifying Official shall ensure that the dependency between the sponsor and family member exists. See paragraphs A.3.3.2.4 and A.5.3.2.5 below.

A5.3.2.4. A valid general or special power of attorney is acceptable if the sponsor is unavailable to sign. Verifying Official will annotate on block 21 the power of attorney presented by the beneficiary.

A5.3.2.5. When the sponsor is unable to sign the DD Form 1172-2 in the presence of the VO, the signature must be notarized. The notary seal / signature should be placed in the right margin of Section II, Block 21.

A5.3.2.6. When the DD Form 1172-2 is not signed in the presence of the authorizing or VO at the time of Defense Enrollment Eligibility Reporting System enrollment, the signature must be notarized. The notary seal and signature should be placed in the right margin of Block 21, above.

A5.3.2.7. 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 Trusted Associate Sponsorship System), formerly, Contractor Verification System.

A5.4.3. Block 26. Sponsoring Office Address. Enter the number and street, city, state, Zone Improvement Plan code, and country code (see Table 6 for country codes and Table 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 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 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. The Department of Defense sponsoring official shall be a uniformed service member, or civilian employee working for the sponsoring organization.

A5.4.16. Block 39. Date Verified. Enter the date 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 are code, prefix, and basic number.

A5.5.4. Block 43. Signature. Verifying Official must sign in the block.

A5.6. SECTION IV – 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. Block 45. Gender. Enter the dependent's gender from the valid codes listed in Table 1 (Use one character.)

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 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

A5.6.5. Block 48. Social Security Number or Department of Defense Identification Number. Enter the dependent's Social Security Number, Department of Defense identification number, ITIN or Temporary Identification Number (TIN). A Temporary Identification Number will automatically be generated by Real-time Automated Personnel Identification System and assigned for categories of beneficiaries who do not yet have Social Security Number s, 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 an Social Security Number is not provided within 270 days. For initial enrollment a Social Security Number, ITIN or Temporary Identification Number is preferred, and an alternate should not be used unless the Social Security Number, ITIN or Temporary Identification Number 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 us for benefits notifications (18 and above)" to verify permission for Department of Defense to contact the included email address with Department of Defense 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 U.S. 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). 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 IV – RECEIPT.

A5.7.1. Block 72. Signature. ID card recipient must sign in that block. If the recipient is incapable of signing, the condition must be indicated in that block.

A5.7.2. Block 73. Date Issued. Enter the date 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.

DD FORM 1172-2, APPLICATION FOR IDENTIFICATION CARD/DEERS ENROLLMENT, APR 2012.

Refer to http://www.cac.mil/

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 http://www.dtic.mil/whs/directives/infomgt/forms/ for DD Form 577 and instructions.

Attachment 7

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

The DD Form 2841 is digitally produced by the Real-time Automated Personnel Identification System workstation and the subscriber (Common Access Card recipient who is a Local Registration Authority/Verifying Official) digitally signs the form by entering their Personal Identification Number.

Attachment 8

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

The DD Form 2842 is digitally produced by the Real-time Automated Personnel Identification System workstation and the subscriber (Common Access Card recipient) digitally signs the form by entering their Personal Identification Numbers.

Attachment 9

RETURNING COMMON ACCESS CARD TO DEFENSE MANPOWER DATA CENTER SUPPORT CENTER

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

A9.2. Returning Common Access Cards by FedEx.

A9.2.1. All Common Access Cards must be returned by FedEx using the D/R account number so your site will not incur associated shipping costs. **Note:** This account is monitored and should not be used to forward the Department of Defense 1172-2 form or for any maintenance actions. All other uses are prohibited. If you have further questions please contact the Defense Manpower Data Center Support Center at 1-800-3RAPIDS or 1-800-372-7473.

A9.2.2. Follow the steps below to complete a Common Access Card 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
1600 North Beauregard Street, Suite 100
Alexandria, VA 22311

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 Common Access Cards being returned and your site's
contact information.

A9.2.2.7. Place returned Common Access Cards, individual Common Access Card Return Forms for each Common Access Card, 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.

Attachment 10

REAL TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM SITE SECURITY MANAGER/VERIFYING OFFICIAL/ IO PROCEDURES FOR LOST, STOLEN, OR DESTORYED 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. This documentation must be scanned and stored in Defense Enrollment Eligibility Reporting System. 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:
A10.1. Lost – report loss to his /her security office or appropriate sponsor agency and request lost application, memorandum, counseling statement, or report.	A10.1. Accept lost application, memorandum, counseling statement, or report from card holder and scan into D/R. See Attachment 11 for sample memorandum.
A10.2. Stolen – report theft to his /her security office or appropriate sponsor agency and request theft application, memorandum, or report.	A10.2. Accept theft application, memorandum, or report from card holder and scan into D/R. See Attachment 11 for sample memorandum.
A10.3. Destroyed - report destruction to his /her security office or appropriate sponsor agency and request destruction application, memorandum, or report, unless damaged Common Access Card is in possession of holder and presented to IO.	A10.3. Accept destruction application, memorandum, or report from card holder and scan into D/R. See Attachment 11 for sample memorandum.
A10.4. 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.	A10.4. Accept application, memorandum, or report and scan into D/R. 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, Coast Guard Common Access Card recipients must present a memorandum (in accordance with the above sample) on Coast Guard letterhead and signed by the Commanding Officer or Officer-in-Charge.

(2) Air Force - Common Access Card 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 Air Force letterhead from the recipient's Commanding Officer, Officer-in-Charge, or Noncommissioned Officer for military, COR or Trusted Agent for contractors, and Supervisor/Division for civilians.

(3) Army - Common Access Card 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 memorandum (in accordance with the above sample) from the individual's Commanding Officer, Officer-in-Charge, or

Noncommissioned Officer for military, COR, Supervisor /Division Chief for civilians/ contractors.

(4) Navy – Common Access Card 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 for civilians.

(5) Marine Corps - Common Access Card 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 for civilians.

(6) Public Health Service - Common Access Card 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 - Common Access Card 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 National Oceanic and Atmospheric Administration letterhead from the recipient's Commanding Officer, Officer-in-Charge for uniformed service personnel, COR, and Supervisor /Division 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

TRUSTED ASSOCIATE SPONSORSHIP SYSTEM, DEFENSE BIOMETRIC IDENTIFICATION SYSTEM, DEFENSE NATIONAL VISTOR 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. Trusted Associated Sponsorship System. Formerly the Contractor Verification System, Trusted Associate Sponsorship System will serve as the vehicle to establish a record into Defense Enrollment Eligibility Reporting System for eligible Department of Defense and uniformed Services contractors and eligible non-DoD populations, in an effort to maintain the integrity of Defense Enrollment Eligibility Reporting System and to ensure physical and logical security in compliance with Homeland Security Presidential Directive-12 standards. Trusted Associate Sponsorship System is a web portal for the verification of contractors by Government Sponsors for the purpose of issuing Common Access Cards. Trusted Associate Sponsorship System replaces the existing 1172-2 paper forms with a web interface and database for tracking the request process and updating Defense Enrollment Eligibility Reporting System with Department of Defense contractor, federal agency personnel, and volunteer/intern population information required for Common Access Card 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 Common Access Cards do not remain active when not appropriate.

A12.1.1. Refer to uniformed Services and Department of Defense 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 Defense Manpower Data Center Trusted Associate Sponsorship System User Guides.

A12.1.2. Trusted Associate Sponsorship System is not designed for the purposes of tracking populations and is a registration and enrollment function of the Defense Enrollment Eligibility Reporting System program. Agencies or units seeking to track certain populations enrolled in Defense Enrollment Eligibility Reporting System must find other alternatives or means of accountability.

A12.2. Defense Biometric Identification System. Defense Biometric Identification System is a Department of Defense identity authentication and force protection tool that is fully operational at selected military locations around the world. Developed by Defense Manpower Data Center, Defense Biometric Identification System serves as a physical access control and critical property registration system, using barcodes and biometrics to identify cardholders. Defense Biometric Identification System implements the policies outlined in DoD Directive 5200.8 and DoD Directive 8190.3 and is an approved system. Defense Biometric Identification System is authorized to issue Department of Defense identity credentials for those individuals needing physical access and not otherwise eligible for a Common Access Card.

A12.2.1. As Department of Defense's largest physical access control system, Defense Biometric Identification System 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 Common Access Cards, Defense Biometric Identification System also verifies authorizations and assigns access privileges based on identity, affiliation and the current threat level. Unlike the "flash pass" method, Defense Biometric Identification System reveals phony and expired identification cards and anyone unauthorized to access military installations. Defense Biometric Identification System 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 Department of Defense facilities to authenticate Department of Defense Common Access Card-carrying visitors using a web-based connection. Defense National Visitors Center is available to Department of Defense law enforcement and force protection elements and is recognized as an approved system under Department of Defense Directive 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 Common Access Cards between participating Federal Agencies and private sector business partners. Use of a federated identity system for recognition of Common Access Card shall strengthen the security of the Department of Defense. Defense Cross-Credentialing Identification System is an approved system under the Personal Identity Protection program.

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

A12.6. Common Access Card Personal Identification Numbers Reset. Common Access Card holders who forget their Personal Identification Number or lock their Common Access Card by entering an incorrect Personal Identification Numbers three successive times need a convenient way to reset their Personal Identification Number. The Common Access Card Personal Identification Numbers Reset system was developed as an alternative to the Real-time Automated Personnel Identification System workstation. Provides a flexible, single-purpose system, for timely Personal Identification Number reset capability for unlocking Common Access Cards, and allows installations the flexibility to position Common Access Card Personal Identification Numbers Reset terminals to best support the needs of their Common Access Card

users. The Common Access Card Personal Identification Numbers Reset process requires the appointment of Trusted Agent Security Managers and Common Access Card Personal Identification Numbers Reset Trusted Agents (CTAs). Trusted Agent Security Managers are responsible for the overall management of Common Access Card Personal Identification Numbers Reset workstations under their purview. CTAs reset Common Access Card Personal Identification Numbers.

A12.7. Volunteer Logical Access Credential. USD (P&R) Memorandum, August 14, 2008, authorizes Department of Defense to initiate D/R as the platform for issuing a logical access credentials to perform volunteer/intern duties. Refer to NIPRNet Enterprise Alternative Token System. The credential is valid for three years, and will have Department of Defense Public Key Infrastructure certificates (identity, email encryption, email digital signing, and Personal Identity Verification Authentication) for authentication to Department of Defense 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 no longer in use. Individuals who receive Volunteer Logical Access Credential access must agree in writing, e.g., digital signature on the DD Form 2842, to be subject to all Department of Defense issuances that govern logical access.

A12.7.1. The volunteer or intern must:

A12.7.2. Be an authorized Department of Defense volunteer (10 United States Code, Section 1588 as implemented in DoDI 1100.21) or student intern (5 United States Code, Section 3111). **Note:** Refer to Agency and Service specific implementation guidance for other eligible populations affiliated with the Volunteer Logical Access Credential program.

A12.7.3. Require frequent access to a Department of Defense network to perform their volunteer duties.

A12.7.4. Be a U.S. citizen.

A12.7.5. Be registered in Defense Enrollment Eligibility Reporting System through the Trusted Associate Sponsorship System, formerly the Contractor Verification System.

A12.7.6. Receive a favorable National Agency Check as required by DoD 5200.2R for individuals requiring network access for Automated Data Processing (ADP)-III positions. **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 Department of Defense sponsored unclassified network account.

A12.7.8. Agree to be photographed and have his/her fingerprints captured and stored in Defense Enrollment Eligibility Reporting System.

A12.8. milConnect. Department of Defense associates and beneficiaries (includes sponsors and family members), manage their personal data and benefits for the Defense Enrollment Eligibility Reporting System program. Individuals sign in to update personal information to the Department of Defense 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, Real-time Automated Personnel Identification System, TRICARE, and other Department of Defense sites provides 24x7 answers to individual benefits questions.

A12.9. ID Card Office Online. Allows self-service options via the Real-time Automated Personnel Identification System Self-Service for making elections to change or update Defense Enrollment Eligibility Reporting System records, renew/replace family ID cards. See Real-time Automated Personnel Identification System Self-Service.

A12.10. NIPRNet 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 Common Access Card. NIPRNet Enterprise Alternative Token System improves security by providing the Public Key Infrastructure authentication credentials to replace user name and password. It strengthens accountability across the NIPRNet by tracking access to these Public Key Infrastructure credentials.