whose visit status and background investigation has been confirmed, documented, and processed in accordance with DoD Directive 5230.20, ''Visits and Assignments of Foreign Nationals'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/523020p.pdf*).

(iii) In accordance with FIPS Publication 201–2, electronically capture and store source documents in the identity-proofing process at the accession points for eligible ID card holders.

(iv) Implement modifications to the CAC applets and interfaces, add contactless capability to the CAC platform and implement modifications to the CAC topology to support compliance with FIPS Publication 201–2.

(v) Establish and implement procedures for capturing biometrics required to support CAC issuance, which includes fingerprints and facial images specified in FIPS Publication 201–2 and National Institute of Standards and Technology Special Publication 800–76–1, ''Biometric Data Specification for Personal Identity Verification'' (available at *http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf*).

(vi) In coordination with the Executive Manager for DoD Biometrics and the Office of the USD(AT&L), implement the capability to obtain two segmented images (primary and secondary) fingerprint minutiae from the full 10-print fingerprints captured as part of the initial background investigation process for CAC issuance.

(vii) Maintain a capability for a CAC holder to reset or unlock PINs from a system outside of the CAC issuance infrastructure.

(2) The Executive Manager for DoD Biometrics, as appointed by the Secretary of the Army as DoD Executive Agent for DoD Biometrics in accordance with DoD Directive 8521.01E, ''Department of Defense Biometrics'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/852101p.pdf*), shall:

(i) Establish biometric standards for collection, storage, and subsequent transmittal of biometric information in accordance with DoD Directive 8521.01E (available at *http://www.dtic.mil/whs/directives/corres/pdf/852101p.pdf*).

(ii) In coordination with the USD(P&R), the USD(I), and the Heads of the DoD Components, establish capability for biometric collection and enrollment operations to support CAC issuance in accordance with 32 CFR part 310 and National Institute of Standards and Technology Special Publication 800–76–1 (available at *http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf*).

(3) The Identity Protection and Management Senior Coordinating Group shall:

(i) Monitor the CAC and identity management related activities outlined within this Instruction in accordance with DoD Instruction 1000.25 (available at *http://www.dtic.mil/whs/directives/corres/pdf/100025p.pdf*).

(ii) Maintain a configuration management process for the CAC and its related components to monitor DoD compliance with FIPS Publication 201–2.

[79 FR 709, Jan. 6, 2014, as amended at 81 FR 74878, Oct. 27, 2016]

Subpart B—DoD Identification (ID) Cards: ID Card Life-Cycle

§ 161.7 ID card life-cycle procedures.

(a) *Sponsorship and eligibility*. In accordance with this part, sponsorship shall incorporate the processes for confirming eligibility for an ID card. The sponsor is the person affiliated with the DoD or other Federal agency who takes responsibility for verifying and authorizing the applicant's need for an ID card. Applicants for a CAC shall be sponsored by a DoD Government official or employee.

(1) The population categories and specific ID cards for which applicants are eligible are listed in Appendix 1 of this section. The majority of these populations are eligible to be sponsored for an ID card based on either their employment status with the DoD or their authorization to receive DoD benefits and entitlements. Examples of these population categories include, but are not limited to: Uniformed services personnel; DoD civilian employees; military retirees; certain DoD beneficiaries; and the eligible dependents for these categories.

(2) Specific populations, listed in paragraph (c)(2)(ii) of Appendix 1 of this section who are eligible to submit

for the ''U.S. DoD/Uniformed Service ID Card'' may only be sponsored if they meet additional criteria. Examples of these population categories include DoD contractors, non-DoD Federal civilians, State employees, and other non-DoD personnel that have an affiliation with the DoD other than through employment or contract. Eligibility for these approved population categories is based on the DoD Government sponsor's determination of the type and frequency of access required to DoD facilities or networks. For the populations described in this paragraph, the applicant's sponsor must confirm that the applicant meets one of the requirements in paragraphs (a)(2)(i) and (iii) of this section:

(i) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely. Access to the DoD network must require the use of a computer with Government-controlled configuration or use of a DoD-approved remote access procedure in accordance with the Defense Information Systems Agency Security Technical Implementation Guide, ''Secure Remote Computing'' (available at *http://iase.disa.mil/stigs/a-z.html* under ''Remote. . .'').

(ii) Remote access, via logon, to a DoD network using DoD-approved remote access procedures.

(iii) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD (applicable to DoD contractors only) on a recurring basis for a period of 6 months or more.

(A) The frequency of ''recurring basis'' for access shall be determined by the DoD Component concerned in coordination with installation security policies.

(B) CAC eligibility for applicants requiring physical access to multiple DoD facilities on a recurring basis for less than 6 months are risk-based decisions that shall be made by the DoD Component concerned in coordination with installation security policies. These applicants may instead be eligible for local or regional base passes in accordance with Office of the Under Secretary of Defense for Intelligence (USD(I)) and local installation security policies and procedures.

(b) *Registration and enrollment.* In accordance with this part, sponsorship and enrollment information about the ID card applicant shall be registered in the DEERS prior to card issuance.

(1) For uniformed services personnel and DoD civilians, all submissions to DEERS must be made electronically via an authorized data source feed (e.g., Civilian Personnel Management Service). Data source feeds for additional population categories shall be approved and incorporated by the Office of the USD(P&R) (OUSD(P&R)) as they become available.

(2) The population categories that are not registered via an authorized data source feed will be registered in DEERS via the RAPIDS using the DD Form 1172–2 or via the TASS (formerly known as CVS, as described in §161.8 of this subpart.

(c) *Background Investigation.* In accordance with this subpart and DoDI 5200.46, ''DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)'' (available at: *http://www.dtic.mil/whs/directives/corres/pdf/ 520046p.pdf*), a background investigation is required for those individuals eligible for a CAC. A background investigation is not currently required for those eligible for other forms of DoD ID cards. The use of the CAC, as the DoD Federal personal identity verification (PIV) card, is governed and supported by additional policies when compared to non-CAC ID cards. Sponsored CAC applicants shall not be issued a CAC without the required background investigation stipulated in DoDI 5200.46 and FIPS Publication 201–2.

(1) A background investigation shall be initiated by the sponsoring organization before a CAC can be issued. The mechanisms required to verify completion of background investigation activities for DoD, military, and civilian CAC populations are managed within the DoD human resources and personnel security communities and are linked to the CAC issuance process. An automated means is not currently in place to confirm the vetting for populations other than DoD military and civilian personnel such as CAC-eligible

contractors and non-DoD Federal civilian affiliates. When data is not available within the CAC issuance infrastructure on the background investigation status for an applicant, the sponsor shall be responsible for confirming that the required background investigation procedures comply with the DoD Instruction 5200.46 and FIPS Publication 201–2 before a CAC is authorized for issuance.

(2) Issuance of a CAC requires, at a minimum, the completion of the Federal Bureau of Investigation (FBI) fingerprint check with favorable results and successful submission of a NACI (or investigation approved in Federal Investigative Standards) to the Office of Personnel Management (OPM). Completed background investigations for CAC issuance shall be adjudicated in accordance with DoD Instruction 5200.46 and Office of Personnel Management Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12'' (available at *http://www.opm.gov/investigate/resources/final_credentialing_standards.pdf*).

(3) Except for uniformed services members, special considerations for conducting background investigations of non-U.S. nationals are addressed in DoD Instruction 5200.46. Non-U.S. person CAC applicants that do not meet the criteria to complete a NACI (e.g., U.S. residency requirements), must meet one of the criteria in paragraph (c)(3)(i) or (ii) of this section prior to CAC issuance. CACs issued to these non-U.S. persons shall display a blue stripe as described in appendix 2 of this section. Procedures for the acceptance of this CAC shall be in accordance with DoD Instruction 5200.46 and Office of Personnel Management Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12.'' The specific background investigation conducted on the non-U.S. person may vary based on governing international agreements. Non-U.S. persons must:

(i) Possess (as foreign military, employee, or contract support personnel) a visit status and security assurance that has been confirmed, documented, and processed in accordance with international agreements pursuant to DoD Directive 5230.20, ''Visits and Assignments of Foreign Nationals'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/ 523020p.pdf*).

(ii) Meet (as direct or indirect DoD hire personnel overseas) the investigative requirements for DoD employment as recognized through international agreements pursuant to Volume 1231 of DoD Instruction 1400.25, ''DoD Civilian Personnel Management System: Employment of Foreign Nationals'' (available at *http://www.dtic.mil/whs/directives/corres/html/CPM_table2.html*). In addition to these investigative requirements, a fingerprint check against the FBI criminal history database, an FBI investigations files (name check search), and a name check against the Terrorist Screening Database shall be required prior to CAC issuance in accordance with Office of Personnel Management Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12.''

(d) *Identity and eligibility verification.* In accordance with this part, identity and eligibility verification shall be completed at a RAPIDS workstation. VOs shall inspect identity and eligibility documentation and RAPIDS shall authenticate individuals to ensure that ID cards are provided only to those sponsored and who have a current affiliation with the DoD. RAPIDS shall also capture uniquely identifying characteristics that bind an individual to the information maintained in DEERS and to the ID card issued by RAPIDS. These characteristics may include, but are not limited to, digital photographs and fingerprints.

(1) *Identity documents.* Applicants for initial ID card issuance shall submit two identity documents in original form as proof of identity. A VO at a RAPIDS workstation shall inspect and verify the documents presented by the applicant before ID card issuance. The identity documents must come from the list of acceptable primary and secondary documents included in the FIPS Publication 201–2 PIV Identity Proofing and Registration Requirements, or, for non-U.S. persons, other sources as outlined within paragraph (d)(1)(ii) of this section. Copies of the

identity documentation may be accepted so long as they are certified documents. In accordance with FIPS Publication 201–2 PIV Identity Proofing and Registration Requirements, the identity documents shall be neither expired nor cancelled. The primary identity document shall be a State or Federal Government-issued picture ID. The identity documents shall be inspected for authenticity and scanned and stored in the DEERS in accordance with the DMDC, ''Real-time Automated Personnel Identification System (RAPIDS) User Guide'' upon issuance of an ID card. The requirement for the primary identity document to have a photo cannot be waived for initial ID card issuance, consistent with applicable statutory requirements. Identity documentation requirements for renewal or re-issuance are provided in paragraph (e)(3) of this section. When it has been determined that a CAC applicant has purposely misrepresented or not provided the applicant's true identity, the case shall be referred by the relevant RAPIDS Service Project office (SPO) to the sponsoring DoD or other Uniformed Service Component organization. The DoD or other Uniformed Service Component organization concerned shall initiate an investigation or provide appeals procedures as appropriate. Exceptions to the identity documentation requirements for initial ID card issuance are provided in paragraphs (d)(1)(i) and (ii) of this section:

(i) *Children*. Children under the age of 18 applying for a dependent ID card are only required to provide documentation for the initial verification of eligibility or proof of relationship to the sponsor described in paragraph (d)(2) of this section.

(ii) *Documentation for non-U.S. persons*. At foreign locations, eligible non-U.S. persons may not possess identity documentation from the FIPS Publication 201–2 PIV Identity Proofing and Registration Requirements required for ID card issuance. These individuals shall still provide personal ID as required by the intent of this paragraph (d)(1). Non-U.S. persons within the continental United States (CONUS) shall present a valid (unexpired) foreign passport as the primary form of identity source documentation. DoD organizations based outside the CONUS should work with the local consular affairs office to determine guidelines for the appropriate identity documentation for eligible non-U.S. persons in accordance with agreements with host nations. It is recommended that a foreign passport be used as the primary form of identity source documentation for these individuals. The requirement for the primary identity document to have a photo cannot be waived. Additional documentation used to verify identity must be original or certified true copies. All documentation not in English must have a certified English translation.

(2) *Eligibility documents*. ID card applicants may be required to provide documentation as initial verification of eligibility for benefits or proof of relationship to the sponsor. The eligibility documents shall be inspected for authenticity by the VO and scanned and stored in DEERS in accordance with the procedures in DMDC, ''Real-time Automated Personnel Identification System (RAPIDS) User Guide.'' Specifications and the types of documents and how they are utilized to verify eligibility for a member or dependent based on their status (e.g., Retired, Reservist, spouse, former spouse, child) shall be established by the uniformed services subject to the guidelines in this subpart. All documentation used to verify eligibility must be original or certified true copies. All documentation not in English must have a certified English translation. Eligibility documentation is not required when DEERS can verify eligibility via an authoritative source or process.

(3) *DEERS verification*. The VO shall utilize DEERS to verify affiliation and eligibility for benefits as described in subpart C of this part.

(4) *Biometrics*. In accordance with DoD Instruction 1000.25, ID card applicants shall provide two fingerprint biometric scans and a facial image, to assist with authenticating the applicant's identity and to bind the information maintained on that individual in DEERS and to the ID card issued by RAPIDS. These requirements shall be integrated into the ID card issuance processes in the following manner:

(i) A digitized, full-face passport-type photograph will be captured for the facial image and stored in DEERS and shall have a plain white or off-white background. No flags, posters, or other images shall appear in the photo. All ID cards issued will display a photograph.

(ii) Two fingerprints are captured for storage within DEERS for applicable ID card applicants. The right and left index fingers shall normally be designated as the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary and secondary designations shall be taken in the following order of priority: Right thumb, left thumb, right middle finger, left middle finger, right ring finger, left ring finger, right little finger, left little finger.

(iii) If two fingerprints cannot be captured, the facial image will be the alternative for authenticating ID card applicants and ID card holders during the issuance process. Additionally, when verification or capture of biometrics is not possible, authorization will be provided by the RAPIDS SSM's digital signature. This transaction shall be subject to audit by DMDC and the uniformed services.

(e) *Issuance.* In accordance with this part, ID cards shall be issued at the RAPIDS workstation after all sponsorship, enrollment and registration, background investigation (CAC only), and identity and eligibility verification requirements have been satisfied. Initial issuance of an ID card to an applicant will be contingent on satisfying the criteria in paragraphs (a) through (d) of this section.

(1) *Cross-servicing.* The uniformed services agree to cross-service the issuance of ID cards when affiliation and eligibility can be verified in DEERS. When eligibility cannot be verified through DEERS, presentation of documentation shall be required. The uniformed services shall restrict cross-servicing for verification of the DD Form 1172–2 and eligibility documentation to the parent uniformed service for the categories in paragraphs (e)(1)(i) through (viii) of this section:

(i) Initial application for permanently incapacitated individuals over age 21 and temporarily incapacitated children over age 21.

(ii) All dependent parents and parents-in-law.

(iii) Illegitimate child of a male sponsor, whose paternity has not been judicially determined.

(iv) Illegitimate child of spouse or sponsor.

(v) Unremarried and unmarried former spouses applying for initial issuance of an ID card.

(vi) Retiree from other services, and former members not currently enrolled in DEERS.

(vii) Surviving dependents of Reserve Retirees on the sponsor's 60th birthday.

(viii) Abused dependents.

(ix) Wards.

(2) *Expiration dates*—(i) *CACs.* Except as noted in paragraphs (e)(2)(i)(A) and (B) of this section, CACs shall be issued for a period not to exceed 3 years from the date of issuance or contract expiration date, whichever is shorter. Unfunded contract options shall be considered in the determination of the length of contract. For example, a contractor hired under DoD contract with a base year plus 2 option years shall be issued a CAC with a 3-year expiration. The expiration date of the PKI certificates on the CAC shall match the expiration date on the card.

(A) CACs issued to DoD civilian employees, contractors, and other eligible personnel assigned overseas or deploying in support of contingency operations shall have an expiration date coinciding with their deployment period end date.

(B) Service Academy students shall be issued 4-year cards with 3-year certificates.

(ii) *Non-CAC ID cards.* (A) DD Form 1173, ''United States Uniformed Services ID and Privilege Card'' issued to dependents of DoD civilian employees, contractors, and other eligible personnel assigned overseas or deploying in support of contingency operations shall have an expiration date coinciding with their deployment period end date.

(B) An indefinite DD Form 1173 will be issued to a dependent of retired Service members who are either 75

years of age or permanently incapacitated in accordance with 10 U.S.C. 1060b.

(C) All other non-CAC ID cards shall be given expiration dates in accordance with the guidance listed on *www.cac.mil*.

(3) *Renewal and reissuance.* Consistent with applicable law, the applicant for ID renewal or reissuance shall be required to surrender the current DoD ID card that is up for renewal or reissuance except as indicated for lost and stolen ID cards in paragraph (e)(3)(iii) of this section. To authenticate renewal or reissuance applicants, the VO shall visually compare the applicant against the facial image stored in DEERS. For applicants who have fingerprint biometrics stored in DEERS, live fingerprint biometrics samples shall be checked against the applicant's DEERS record. If the biometric check confirms the identity of the renewal or reissuance applicant then no additional documentation is required to verify identity other than the ID card that is being renewed or reissued (documentation may still be required to verify or re-verify eligibility as described in paragraph (d)(2) of this section). As a general practice for renewal or re-issuance, two fresh fingerprint biometric captures may be stored for applicable personnel through the initial procedures in paragraph (d)(4)(ii) of this section to support DMDC's biometric update schedule.

(i) An ID card holder may apply for a renewal starting 90 days prior to the expiration of a valid ID. The SPO can provide exceptions to this requirement.

(ii) An ID card shall be reissued when printed information requires changes (e.g., pay grade, rank, change in eligibility), when any of the media (including printed data, magnetic stripe, bar codes, or integrated circuit chip) becomes illegible or inoperable, or when a CAC is known or suspected to be compromised.

(iii) An ID card shall be reissued when it is reported lost or stolen. The individual reporting a lost or stolen ID card shall be required to provide a valid (unexpired) State or Federal Government-issued picture ID as noted in paragraph (d)(1) of this section, consistent with applicable law, when available. If the individual is unable to present the required identity documentation, a biometric verification shall be used as proof of identity as described in paragraph (e)(3)(iii)(A) of this section. The VO shall verify the cardholder's identity against the biometric information stored in DEERS and confirm the expiration date of the missing ID card. 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 DEERS. For dependents, the DD Form 1172–2 serves as the supporting documentation for a lost or stolen card. For individuals sponsored through TASS, the replacement ID card shall have the same expiration date as the lost or stolen card.

(A) If no identity documentation is available but biometric information (facial image or fingerprint when applicable) in the DEERS database can be verified by the VO, an ID card can be reissued to the individual upon the additional approval of a SSM. This transaction shall be digitally signed and audited.

(B) If biometric information cannot be verified, the requirements for initial issuance shall apply or a temporary card may be issued in accordance with paragraph (e)(4) of this section.

(4) *Temporary cards*—(i) *Temporary issuance of a CAC.* During contingency operations, in the event there is no communication with the DEERS database or the certificate authority, a temporary CAC may be issued with an abbreviated expiration date for a maximum of 10 days. The temporary card will not have PKI certificates and will be replaced as soon as the member can reach an online RAPIDS station or communications have been restored. Additionally, the temporary CAC does not communicate or imply eligibility to any DoD benefit. This capability will be enabled only at affected RAPIDS sites and must have approval granted by DMDC.

(ii) *Temporary issuance of a Uniformed Services Identification card.* There are multiple scenarios under which a temporary Uniformed Services Identification card may be issued. The uniformed

services shall develop standard processes and procedures for scenarios requiring issuance of a temporary DD Forms 2765 ''Department of Defense/Uniformed Services Identification and Privilege Card'' or DD 1173, including but not limited to those situations where the applicant needs to obtain the necessary legal documentation or the sponsor is unavailable to provide an authorizing signature.

(5) *Multiple cards.* Individuals shall be issued a separate ID card for each population category for which they qualify as described in Appendix 1 of this section. In instances where an individual has been issued more than one ID card (e.g., an individual that is eligible for an ID card as both a Reservist and as a DoD contractor employee), only the ID card that most accurately depicts the capacity in which the individual is affiliated with the DoD should be utilized at any given time.

(f) *Use and maintenance.* In accordance with this part, ID cards shall be used as proof of identity and DoD affiliation to facilitate access to DoD facilities and systems. Additionally, ID cards shall represent authorization for entitled benefits and privileges in accordance with DoD policies. The CAC, as the DoD Federal PIV card, is governed and supported by additional policies and infrastructure when compared to non-CAC ID cards. This section provides additional guidance on CAC use and maintenance:

(1) *Access.* The granting of access privileges is determined by the facility or system owner as prescribed by the DoD.

(2) *Accountability.* CAC holders will maintain accountability of their CAC at all times while affiliated with the DoD.

(3) *PKI.* Using the RAPIDS platform, DoD PKI identity and PIV authentication certificates will be issued on the CAC at the time of card issuance in compliance with OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12.'' Email signature, email encryption, or PIV authentication certificates may also be available on the CAC either upon issuance or at a later time. If the person receiving a CAC does not have an organization email address assigned to them, they may return to a RAPIDS terminal or use milConnect to receive their email certificate when the email address has been assigned. To help prevent inadvertent disclosure of controlled information, email addresses assigned by an organization shall comply with DoD Instruction 8500.2, ''Information Awareness (IA) Implementation'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/ 850002p. pdf*).

(4) *milConnect.* DoD has a self-service Web site available that allows an authenticated CAC holder to add applets to the CAC, change the email address, add/update Email Signature and Email Encryption Certificates, and activate the Personal Identity Verification (PIV) Authentication certificate. This capability can be utilized from any properly configured UNCLASSIFED networked workstation. The milConnect Web site is *https://www.dmdc.osd.mil/milconnect.*

(5) *CAC Personal ID Number (PIN) Reset.* DoD has manned workstations capable of resetting the PINs of a CAC holder with a locked card or forgotten PIN. These workstations are intended to provide alternative locations for CAC holders to service their cards other than RAPIDS issuance locations. To authenticate cardholders, live biometric samples shall be checked against the biometrics stored in DEERS prior to resetting CACs. This process requires the presence of a CPR trusted agent (CTA) or TASM or RAPIDS VO or SSM.

(g) *Retrieval and revocation.* In accordance with this part, ID cards shall be retrieved by the sponsor or sponsoring organization when the ID card has expired, when it is damaged or compromised, or when the card holder is no longer affiliated with the DoD or no longer meets the eligibility requirements for the card. The active status of the card shall be terminated within the DEERS and RAPIDS infrastructure. The CAC, as the DoD Federal PIV card, is governed and supported by additional policies and infrastructure when compared to non-CAC ID cards. This section provides additional guidance on CAC retrieval and revocation:

(1) CACs shall be retrieved as part of the normal organizational or command-level check-out processes. The active status of the CAC shall also be terminated in special circumstances (e.g., absent without leave, unauthorized absence, missing in action) in accordance with organization or command-level security policies.

(2) The DoD sponsor or sponsoring organization is ultimately responsible for retrieving CACs from their personnel who are no longer supporting their organization or activity. CAC retrieval will be documented and treated as personally identifiable information, in accordance with DoD Regulation 5200.1–R, and 32 CFR part 310 and receipted to a RAPIDS site for disposition in a timely manner.

(3) Upon loss, destruction, or revocation of the CAC, the certificates thereon are revoked and placed on the certificate revocation list in accordance with Assistant Secretary of Defense for Networks and Information Integration Certificate Policy, ''X.509 Certificate Policy for the United States Department of Defense'' (available at *http://jitc.fhu.disa.mil/pki/documents/dod_x509_certificate_policy_v9_0_9_february_2005.pdf*). All other situations that pertain to the disposition of the certificates are handled in accordance with Assistant Secretary of Defense for Networks and Information Integration Certificate Policy, ''X.509 Certificate Policy for the United States Department of Defense'' as implemented.

APPENDIX 1 TO § 161.7—ID CARD DESCRIPTIONS AND POPULATION ELIGIBILITY CATEGORIES

(a) *Overview*. Paragraphs (b) through (e) of this appendix contain information on the CAC type of ID card. The remaining paragraphs in the appendix contain information on all other versions of DoD enterprise-wide ID cards. This appendix describes these cards and lists some of the categories of populations that are eligible to be sponsored for the cards under the guidelines described in paragraph (a) of § 161.7; additional ID-card eligible categories are codified in subpart C of this part. RAPIDS accesses DEERS information collected by the DD Form 1172–2 to generate all of the ID Cards identified in this appendix. The benefits and entitlements that support ID card eligibility for populations in this appendix are described in subpart C of this part. Guidelines and restrictions that pertain to all forms of DoD ID cards are included in this part.

(b) *Armed Forces of the United States Geneva Conventions ID Card*—(1) *Description*. This CAC is the primary ID card for uniformed services members and shall be used to identify the member's eligibility for benefits and privileges administered by the uniformed services as described in subpart C of this part. The CAC shall also be used to facilitate standardized, uniform access to DoD facilities, and installations in accordance with Directive Type Memorandum 09–012, ''Interim Policy Guidance for DoD Physical Access Control'' (available at: *http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-012.pdf*) and DoD 5200.08–R, ''Physical Security Program,'' and to computer systems in accordance with DoD Instruction 8520.02, ''Public Key Infrastructure (PKI) and Public Key (PK) Enabling,'' (available at: *http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf*).

(i) The card shall also serve as ID for purposes of Geneva Convention requirements in accordance with DoD Instruction 1000.01.

(ii) If a member is captured as a hostage, detainee, or prisoner of war (POW), the card shall be shown to the capturing authorities, but, insofar as possible, should not be surrendered.

(2) *Eligibility*. Those populations eligible for this type of CAC include:

(i) Members of the regular components of the Military Services.

(ii) Members of the Selected Reserve of the Ready Reserve of the Reserve Components.

(iii) Members of the IRR of the Ready Reserve authorized in accordance with regulations prescribed by the Secretary of Defense to perform duty in accordance with 10 U.S.C. 10147.

(iv) Uniformed services members of NOAA and USPHS.

(c) *U.S. DoD or Uniformed Services ID Card*—(1) *Description*. This CAC is the primary ID card for eligible civilian employees, contractors, and foreign national affiliates and shall be used to facilitate standardized, uniform access to DoD facilities, and installations in accordance with Directive Type Memorandum 09–012, ''Interim Policy Guidance for DoD Physical Access Control'' and DoD 5200.08–R, ''Physical Security Program,'' and computer systems in accordance with DoD Instruction 8520.02, ''Public Key Infrastructure (PKI) and Public Key (PK) Enabling.''

(2) *Eligibility*. (i) DoD civilian employees are eligible for this CAC, to include:

(A) Individuals appointed to appropriated fund and NAF positions.

(B) USCG and NOAA civilian employees.

(C) Permanent or time-limited employees on full-time, part-time, or intermittent work schedules for 6 months or more.

(D) SES, Competitive Service, and Excepted Service employees.

(ii) Eligibility for additional populations shall be based on a combination of the personnel category and the DoD Government sponsor's determination of the type and frequency of access required to DoD networks and facilities described in paragraph (a) of §161.7 of this subpart. These personnel categories include:

(A) Non-DoD civilian employees to include:

(*1*) State employees working in support of the National Guard.

(*2*) IPA employees.

(*3*) Non-DoD Federal employees that are working in support of DoD but do not possess a Federal PIV card that is accepted by the sponsoring DoD Component. DoD Components shall obtain DHRA approval prior to sponsorship.

(B) DoD contractors.

(C) USCG and NOAA contractors.

(D) Persons whose affiliation with DoD is established through:

(*1*) *Direct and Indirect Hiring Overseas*. Non-U.S. citizens hired under an agreement with the host nation and paid directly by the uniformed services (direct hire) or paid by an entity other than the uniformed services for the benefits of the uniformed services (indirect hire).

(*2*) *Assignment as Foreign Military, Foreign Government Civilians, or Foreign Government Contractors to Support DoD Missions*. Non-U.S. citizens who are sponsored by their government as part of an official visit or assignment to work with DoD.

(*3*) *Procurement Contracts, Grant Agreements or Other Cooperative Agreements*. Individuals who have an established relationship between the U.S. Government and a State, a local government, or other recipient as specified in 31 U.S.C. 6303, 6304, and 6305.

(d) *U.S. DoD or Uniformed Services ID and Privilege Card*—(1) *Description*. This CAC is the primary ID card for civilian employees, contractors, and foreign national military, as well as other eligible individuals entitled to benefits and privileges administered by the uniformed services as described in subpart C of this part. The CAC shall be used to facilitate standardized, uniform access to DoD facilities, and installations in accordance with Directive Type Memorandum 09–012, ''Interim Policy Guidance for DoD Physical Access Control'' and DoD 5200.08–R, ''Physical Security Program,'' and computer systems in accordance with DoD Instruction 8520.02, ''Public Key Infrastructure (PKI) and Public Key (PK) Enabling.''

(2) *Eligibility*. Specific population categories are entitled to benefits and privileges, in accordance with subpart C of this part, and shall be eligible for this CAC, to include:

(i) DoD and uniformed services civilian employees (both appropriated and non-appropriated) when required to reside in a household on a military installation within the CONUS, Hawaii, Alaska, Puerto Rico, and Guam.

(ii) DoD and uniformed services civilian employees when stationed or employed and residing in foreign countries for a period of at least 365 days.

(iii) DoD contractors when stationed or employed and residing in foreign countries for a period of at least 365 days.

(iv) DoD Presidential appointees who have been appointed with the advice and consent of the Senate.

(v) Civilian employees of the Army and Air Force Exchange System, Navy Exchange System, and Marine Corps Exchange System and NAF activity employees of the Coast Guard Exchange Service.

(vi) Uniformed and non-uniformed full-time paid personnel of the Red Cross assigned to duty with the uniformed services within the CONUS, Hawaii, Alaska, Puerto Rico, and Guam, when required to reside in a household on a military installation.

(vii) Uniformed and non-uniformed, full-time, paid personnel of the Red Cross assigned to duty with the uniformed services in foreign countries.

(viii) Foreign military who meet the eligibility requirement of paragraph (a)(2) of §161.7 and are in one of the categories in paragraphs (d)(2)(viii)(A) through (C) of this appendix. Those foreign military not meeting the eligibility requirements for CAC as described in paragraph (a)(2) of §161.7 shall be issued a DD Form 2765 as described in paragraph (l) of this appendix.

(A) Active duty officers and enlisted personnel of North Atlantic Treaty Organization (NATO) and Partnership For Peace (PFP) countries serving in the United States under the sponsorship or invitation of the DoD or a Military Department.

(B) Active duty officers and enlisted personnel of non-NATO countries serving in the United States under the sponsorship or invitation of the DoD or a Military Department.

(C) Active duty officers and enlisted personnel of NATO and non-NATO countries when serving outside the United States and outside their own country under the sponsorship or invitation of the DoD or a Military Department, or when it is determined by the major overseas commander that the granting of such privileges is in the best interests of the United States and such personnel are connected with, or their activities are related to, the performance of functions of the U.S. military establishment.

(e) *U.S. DoD or Uniformed Service Geneva Conventions ID Card for Civilians Accompanying the Armed Forces*—(1) *Description*. This CAC serves as the DoD and/or Uniformed Services Geneva Conventions ID card for civilians accompanying the uniformed services and shall be used to facilitate standardized, uniform access to DoD facilities, and installations in accordance with Directive

Type Memorandum 09–012, ''Interim Policy Guidance for DoD Physical Access Control'' and DoD 5200.08–R, ''Physical Security Program,'' and computer systems in accordance with DoD Instruction 8520.02, ''Public Key Infrastructure (PKI) and Public Key (PK) Enabling.''

(2) *Eligibility*. The following population categories are eligible for this CAC:

(i) Emergency-essential employees as defined in DoD Directive 1404.10, ''DoD Civilian Expeditionary Workforce'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/140410p.pdf*).

(ii) Contractors authorized to accompany the force (contingency contractor employees) as defined in Joint Publication 1–02 (available at *http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf*).

(f) *DD Form 2, ''Armed Forces of the United States Identification Card (Reserve).''*—(1) *Description*. This is the primary ID card for RC members not eligible for a CAC. Benefits and privileges shall be administered by the uniformed services as described in subpart C of this part.

(i) The DD Form 2S (RES) shall serve as ID for purposes of the Geneva Convention requirements in accordance with DoD Instruction 1000.01.

(ii) If a member is captured as a hostage, detainee, or POW, the DD Form 2S (RES), shall be shown to the capturing authorities, but, insofar as possible, should not be surrendered.

(2) *Eligibility*. Those populations eligible for the DD Form 2S (RES) include:

(i) Ready Reserve, who are not otherwise entitled to either DD Form 2S (RET), ''Armed Forces of the United States Geneva Conventions Identification Card (Retired) (Blue),'' or a CAC.

(ii) The Standby Reserve.

(iii) The Reserve Officers' Training Corps College Program students that have signed a contract leading to military service.

(g) *DD Form 2S (Ret)*—(1) *Description*. This is the primary ID card for retired uniformed services members entitled to retired pay. Benefits and privileges shall be administered by the uniformed services as described in subpart C of this part.

(2) *Eligibility*. Members of the uniformed services who are entitled and in receipt of retired pay, or entitled and have waived their retired pay, are eligible for the DD 2S (RET).

(h) *DD Form 2, ''United States Uniformed Services Identification Card (Reserve Retired).''*—(1) *Description*. This is the primary ID card for members of the National Guard or Reserves who have completed 20 creditable years of service and have elected to be transferred to the Retired Reserve. They will qualify for pay at age 60, or earlier if they have qualified contingency service.

(2) *Eligibility*. Members of the Reserve Components who are entitled to retired pay at age 60 (or earlier if they have qualified contingency service) and have not yet attained age 60 are eligible for the DD Form 2 (Reserve Retired).

(i) *DD Form 1173*—(1) *Description*. This is the primary ID card for dependents and other similar categories of individuals eligible for benefits and privileges administered by the uniformed services as described in subpart C of this part.

(2) *Eligibility*. Specific population categories entitled to benefits and privileges as described in subpart C of this part are eligible for the DD Form 1173 to include:

(i) Dependents of active duty Service members of the regular components, Reserve Component Service members on active duty for more than 30 days, and retirees.

(ii) Surviving dependents of active duty members.

(iii) Surviving dependents of retired military members.

(iv) Surviving dependents of MOH recipients and surviving dependents of honorably discharged veterans rated by the Department of Veterans Affairs (VA) as 100 percent disabled from a uniformed services-connected injury or disease at the time of his or her death.

(v) Accompanying dependents of foreign military.

(vi) Dependents of authorized civilian personnel overseas.

(vii) Other benefits eligible categories as described in subpart C of this part.

(j) *DD Form 1173–1, ''Department of Defense Guard and Reserve Family Member Identification Card.''*—(1) *Description*. This is the primary ID card for dependents of Ready Reserve and Standby Reserve members not on active duty in excess of 30 days. When accompanied by a set of the sponsor's valid active duty orders, the card shall be used in place of a DD Form 1173 for a period of time not to exceed 270 days, if the member is called to active duty by congressional decree or Presidential call-up under 10 U.S.C. chapter 1209.

(2) *Eligibility*. Eligible dependents of Reserve Component members and retirees as described in subpart C of this part are eligible for the DD Form 1173–1.

(k) *DD Form 2764, ''United States DoD/Uniformed Services Geneva Conventions Card.''*—(1) *Description*. This is the primary ID for non-CAC eligible civilian noncombatant personnel who are deployed in conjunction with military operations overseas. The DD Form 2764 also replaces DD Form 489, ''Geneva Conventions Identity Card for Civilians Who Accompany the Armed Forces.''

(2) *Eligibility*. Civilian noncombatant personnel who have been authorized to accompany U.S. forces in regions of conflict, combat, and contingency operations and who are liable to capture and detention by the enemy

as POWs are eligible for the DD Form 2764 in accordance with DoD Instruction 1000.01.

(l) *DD Form 2765*—(1) *Description*. This is the primary ID card for categories of individuals, other than current or retired members of the uniformed services, who are eligible for uniformed services benefits and privileges in their own right without requiring a current affiliation with another sponsor.

(2) *Eligibility*. Those populations eligible for the DD Form 2765 include:

(i) Foreign national military personnel described in paragraph (d)(2)(viii) of this appendix that cannot meet all criteria for CAC issuance.

(ii) Former members.

(iii) Members eligible for transitional health care (THC). These individuals shall be eligible for DD Form 2765 (with a ''TA'' overstamp) showing expiration date for each benefit, as shown on the reverse of the card.

(iv) MOH recipients.

(v) DAV (rated 100 percent disabled by the Department of Veterans Affairs).

(vi) Former spouse (that qualify as a DoD beneficiary).

(vii) Civilian personnel in the categories listed in paragraphs (l)(2)(vii)(A) through (D) of this appendix:

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

(B) Area executives, center directors, and assistant directors of the United Service Organization, when serving in foreign countries.

(C) United Seaman's Service (USS) personnel in foreign countries.

(D) Military Sealift Command (MSC) civil service marine personnel deployed to foreign countries on MSC-owned and -operated vessels.

(m) *DoD Civilian Retiree Card*—(1) *Description*. This ID shall only be used to establish DoD civilian retiree identity and affiliation with the DoD.

(2) *Eligibility*. Appropriated and NAF civilians that have retired from any DoD Service component or agency are eligible for the DoD Civilian Retiree Card. These civilians must have their retired status verified in DEERS before an ID card can be issued.

(n) *NOAA Retired Wage Mariner and Family Member Card*—(1) *Description*. The NOAA Retired Wage Mariner and Family Member Card is a sub-category of the DoD Civilian Retiree Card and shall be used to establish identity and affiliation with the DoD and to identify the individual's eligibility for benefits and privileges administered by the uniformed services as described in subpart C of this part.

(2) *Eligibility*. Retired Wage Mariners of NOAA and their dependents as described in subpart C of this part are eligible for the NOAA Retired Wage Mariners and Family Members Card.

APPENDIX 2 TO §161.7—TOPOLOGY SPECIFICATIONS

(a) *Topology*. Graphical representations of all CACs are maintained at *www.cac.mil*.

(b) *CAC stripe color coding*. The CAC shall be color-coded as indicated in the Table to reflect the status of the holder of the card.

(1) If a person meets more than one condition as shown in the Table, priority will be given to the blue stripe to denote a non-U.S. citizen unless the card serves as a Geneva Conventions card.

(2) FIPS Publication 201–2 reserves the color red to distinguish emergency first responder officials. Until the DoD implementation of Homeland Security Presidential Directive 12 is complete, the color red will also be used to denote non-U.S. personnel in the same manner as the blue stripe in the Table (i.e., some cards with red stripes may continue to exist in circulation until the 3-year life cycle is complete).

TABLE—CAC STRIPE COLOR CODING

No stripe	U.S. military and DoD civilian personnel or any personnel eligible for a Geneva Conventions card
Blue	Non-U.S. personnel, including DoD contract employees (other than those persons requiring a Geneva Conventions card).
Green	All U.S. citizen personnel under contract to the DoD (other than those persons requiring a Geneva Conventions card).

(c) *CAC printed statements*—(1) Eligible individuals who are permanently assigned in foreign countries for at least 365 days (it should be noted that local nationals are in their home country, not a foreign country) will have the word ''OVERSEAS'' printed within the authorized patronage area of the CAC.

(2) The authorized patronage area for eligible individuals permanently assigned within CONUS will be blank. Travel orders authorize access for these individuals while en route to the deployment site.

(3) During a conflict, combat, or contingency operation, civilian employees with a

U.S. DoD or Uniformed Services Geneva Conventions ID Card for Civilians Accompanying the Uniformed Services will be granted all commissary; exchange; MWR; and medical privileges available at the site of the deployment, regardless of the statements on the ID card. Contractor employees possessing this ID card shall receive the benefit of those commissary, exchange, MWR, 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.

(4) The medical area on the card for individuals on permanent assignment in a foreign country will contain the statement: ''When TAD/TDY or stationed overseas on a space available fully reimbursable basis.'' However, civilian employees and contractor employees providing support when forward deployed during a conflict, combat, or contingency operation are treated in accordance with 10 U.S.C. 10147 and chapters 1209 and 1223 and DoD Instruction 3020.41, ''Operational Contract Support'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/302041p.pdf*), and the 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'' (available at *http://cpol.army.mil/library/nonarmy/dod_092407.pdf*).

(d) *Blood type indicators.* A blood type indicator is an optional data element on the ID card and will only appear on the card if the blood type is provided by an authoritative data source prescribed by TRICARE Management Activity.

(e) *Organ donor indicators.* An organ donor indicator is an optional data element on the ID card and will only appear if the card applicant opts for this feature at the time of card issuance.

[79 FR 709, Jan. 6, 2014, as amended at 81 FR 74878, Oct. 27, 2016]

§ 161.8 ID card life-cycle roles and responsibilities.

(a) *General.* This section provides the roles and responsibilities associated with a series of processes and systems that support the ID card life-cycle. The requirements provided in this section may be supplemented by military Service guidance, DoD Component-level procedures and DMDC procedural and system documentation on DEERS, RAPIDS, TASS, and CPR.

(b) *Separation of duties.* The ID card life-cycle includes a requirement for a separation of duties to support the issuance process. This rule requires more than one person to serve in an official role during the sponsorship and enrollment and issuance processes. Authorizing a RAPIDS SSM or VO to exercise the duties of a TASS TASM, TA, or sponsor would allow a single individual to control the ID card issuance process, from record creation to card issuance. Individuals serving in the role of a RAPIDS SSM or VO shall not exercise the role of the TASS TASM or TA or the role of the signatory sponsor on the DD Form 1172–2. (In the case of their own dependents, a RAPIDS SSM or VO can serve as the sponsor on the DD Form 1172–2 but cannot serve as the VO for card issuance.)

(c) *DD Form 1172–2.* The DD Form 1172–2 shall be used to collect the information necessary to register ID card and CAC applicants in DEERS via RAPIDS who are not enrolled through an authorized personnel data feed or are not registered through TASS. The DD Form 577, ''Appointment/Termination Record—Authorized Signature,'' shall be used to verify the sponsoring individual's signature, when verification through RAPIDS is unavailable. This form is to be used primarily for DEERS enrollment and verification of initial and continued association for dependents and DoD affiliates (e.g., foreign national military). The DD Form 1172–2 shall also be used to add benefits conditions for eligible personnel in accordance with DMDC, ''Real-time Automated Personnel Identification System (RAPIDS) User Guide'' and subpart C of this part. Retention and disposition of the DD Form 1172–2 shall be in accordance with the uniformed services' regulatory instructions. In the absence of electronic verification of sponsorship for the enrollment or reenrollment of dependents, the sponsor signing block 65 in Section 5 of the DD Form 1172–2 for the ID card applicant:

(1) Shall be a uniformed services member, retiree, civilian employee working for the sponsoring organization, or an individual entitled to DoD benefits in their own right, without requiring relationship to another sponsor, as described in subpart C of this part.

(2) Must be a DoD ID card or CAC holder.