



PERSONNEL AND
READINESS

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

December 1, 2008

Incorporating Change 3, September 27, 2011

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance"

References: See Attachment 1

Purpose. This DTM provides interim implementation guidance governing the CAC pursuant to Deputy Secretary of Defense Memorandum (Reference (a)). The Department of Defense is currently migrating to the next generation CAC in order to meet the Federal requirements for credentialing contained within Homeland Security Presidential Directive-12 and Federal Information Processing Standards Publication 201-1 (References (b) and (c)). Migration to the next generation CAC will take place over multiple years as the card issuance hardware and software are upgraded. CACs issued in conjunction with previous CAC policy (Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and DoD Chief Information Officer memorandum (Reference (d)) will remain valid until replaced with the next generation CAC. This DTM shall be incorporated into DoD Manual 1000.13-M, Volume 1, and shall expire effective September 30, ~~2011~~ 2012. Successful migration to the next generation CAC will require coordination and collaboration within and among all CAC communities (e.g., personnel security, operational security, industrial security, information security, physical security, and information technology). Please distribute Attachments 1 through 3 and the Glossary, as appropriate, to the local installations and commands within the Department of Defense.

Applicability. This DTM applies to OSD, the Military Departments (including the U.S. Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

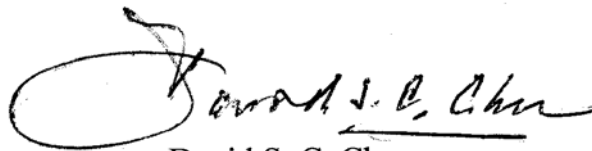
This DTM also applies to the Commissioned Corps of the U.S. Public Health Service, under agreement with the Department of Health and Human Services; and the National Oceanic and Atmospheric Administration, under agreement with the Department of Commerce.

Responsibilities. See Attachment 2.

Procedures. The new guidelines are at Attachment 3 and are effective immediately. Implementation should occur as soon as practical, as units begin issuing the next generation CAC.

Releasability. UNLIMITED. This DTM is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.

Point of contact for this memorandum is Ms. Heidi Boyd, (703) 696-0404.

A handwritten signature in black ink, appearing to read "David S. C. Chu". The signature is written in a cursive style with a large, looped initial "D".

David S. C. Chu
Under Secretary of Defense for
Personnel and Readiness

Attachments:
As stated

DISTRIBUTION:

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
COMMANDANT, UNITED STATES COAST GUARD
DIRECTOR, NOAA CORPS
DIRECTOR, UNITED STATES PUBLIC HEALTH SERVICE

ATTACHMENT 1

REFERENCES

- (a) Deputy Secretary of Defense Memorandum, "DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12)," November 26, 2008
- (b) Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- (c) Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006
- (d) Under Secretary Defense for Personnel and Readiness and Department of Defense Chief Information Officer Memorandum, "Common Access Card - Changes," April 18, 2002
- (e) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- (f) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (g) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (h) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
- (i) DoD 5200.1-R, "Information Security Program," January 14, 1997
- (j) Defense Manpower Data Center (DMDC), "DoD Implementation Guide for CAC Next Generation Version 2.6," November 2006¹
- (k) DMDC, "DoD Implementation Guide for CAC PIV End-Point version 1.0," December 17, 2007¹
- (l) DoD 5200.2-R, "Personnel Security Program," January 1987
- (m) DoD 1400.25-M, "Department of Defense Civilian Personnel Manual," December 1996
- (n) Under Secretary of Defense for Personnel and Readiness Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005²
- (o) Office of Management and Budget Memorandum (OMB) 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
- (p) Office of Personnel Management (OPM) Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," July 31, 2008
- (q) Office of Personnel and Management Federal Investigations Notice 06-04, "HSPD-12 – Advanced Fingerprints Results," June 8, 2006
- (r) Real-time Automated Personnel Identification System (RAPIDS) 7.1 User Guide, February 2007³
- (s) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 5, 1997

¹ Available at <http://www.dmdc.osd.mil/smartcard>

² Available from Defense Human Resource Agency at (703) 696-1073.

³ Available from Defense Manpower Data Center Personnel Identity Protection Solutions (PIPS) Division at (703) 696-0036.

- (t) Section 701 of title 18, United States Code
- (u) "X.509 Certificate Policy for the United States Department of Defense," February 9, 2005
- (v) DoD Instruction 1000.1, "Identity Cards Required by the Geneva Conventions," January 30, 1974
- (w) DoD Directive 1404.10, "Emergency - Essential (E-E) DoD U.S. Citizen Civilian Employees," April 10, 1992
- (x) DoD Instruction 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces," October 3, 2005
- (y) Deputy Secretary of Defense Memorandum, "Policy Guidance for Provision of Medical Care for Department of Defense Civilian Employees Injured or Wounded While Forward Deployed in Support of Hostilities," September 24, 2007
- (z) Sections 311, 2102, 2103, 2105, 3132, and 5311-5318 of title 5, United States Code
- (aa) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended
- (ab) Chapter 15, sections 331-335, 688, 1581, 1588, 12301(a), 12032, 12304, 12305, and 12406 of title 10, United States Code

ATTACHMENT 2

RESPONSIBILITIES

1. USD(P&R). The USD(P&R) shall:

a. Develop policy for the CAC, including minimum acceptable criteria for establishment and confirmation of personal identity, policy for the issuance of the DoD enterprise personnel identity credentials, and approval of additional systems under the Personnel Identity Protection (PIP) Program.

b. Act as the Principal Staff Assistant for the Defense Enrollment Eligibility Reporting System (DEERS), Real-time Automated Personnel Identification System (RAPIDS), and the PIP Program in accordance with DoD Directive 5000.01 (Reference (e)). Appoint the designated approving authority for all PIP systems in accordance with DoD Directive 8500.01E (Reference (f)).

c. In coordination with the Under Secretary of Defense for Intelligence, Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, and Under Secretary of Defense for Acquisition, Technology, and Logistics, establish policy and oversight for CAC issuance in compliance with Reference (c).

2. DIRECTOR, DEFENSE MANPOWER DATA CENTER (DMDC). The Director, DMDC, under the authority, direction, and control of the USD(P&R), shall:

a. Develop and field the required DEERS/RAPIDS infrastructure and all elements of field support (including but not limited to software distribution, hardware procurement and installation, on-site and depot level hardware maintenance, on-site user training and central telephone center support, and telecommunications engineering and network control center assistance) to issue the CAC.

b. Procure and distribute consumables, including card stock and printing supplies, commensurate with funding received from the DoD Components.

c. Consistent with applicable law and in coordination with the Under Secretary of Defense for Intelligence (USD(I)), establish interface with OPM for access to the Clearance Verification System for information regarding advanced fingerprint check status and confirmation of background investigation information to issue the Next Generation CAC.

d. In coordination with Under Secretary of Defense for Policy (USD(P)), establish an electronic process for securing CAC eligibility information on foreign military, employee, or contract support personnel whose visit status and background investigation has been adjudicated and approved by the USD(P) according to DoD Directive 5230.20 (Reference (g)).

e. In coordination with and on behalf of the DoD Components, implement a central management and distribution system for electromagnetic opaque sleeves or other comparable technologies that can be provided during the CAC issuance process. This capability is expected to be available in September 2009.

3. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Comply with this policy and distribute this guidance to local and/or regional organizations.

b. Furnish appropriate space and staffing for card issuing operations, as well as reliable telecommunications to and from the Defense Information Systems Agency-managed Unclassified but Sensitive Internet Protocol Router Network (NIPRNet).

c. Provide funding for the cardstock and printer consumables to DMDC.

d. Ensure contract support and other affiliate CAC applicants have met background investigation requirements outlined within paragraph 3.c. of Attachment 3 prior to approving CAC sponsorship and authorization.

e. Establish processes and procedures for collection of the government furnished CACs for all categories of DoD personnel when there is a separation, retirement, or termination. Since CACs contain personal identifiable information (PII), they shall be treated and controlled in accordance with DoD Directive 5400.11 (Reference (h)) and DoD 5200.1-R (Reference (i)). These cards shall be returned to any RAPIDS issuance location for proper disposal.

f. In accordance with FIPS 201, make available electromagnetic opaque sleeves or other comparable technologies to protect against any unauthorized contactless access to the cardholder unique identification number (CHUID) stored on the CAC.

g. Provide oversight of CAC Contractor Verification System (CVS) Trusted Agents (TA) and Trust Agent Security Managers (TASM) and ensure the number of contractors overseen by any TA is manageable.

ATTACHMENT 3

NEXT GENERATION CAC IMPLEMENTATION GUIDANCE

1. BACKGROUND. Reference (b) directed the distribution of a Federal standard for secure and reliable forms of identification for Federal employees and contractors that will be interoperable among the Federal departments and agencies. The resulting standard, Reference (c), defines the requirements for personal identity verification (PIV) credentials that are issued only when an individual's identity and background have been properly vetted and positively adjudicated; are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; and can support rapid electronic authentication.

a. The Department of Defense is migrating the CAC program to meet the requirements in Reference (b). This affects the current CAC-holding population including active duty military personnel, members of the selected Reserve and National Guard, DoD civilian employees, eligible contractor personnel, and other eligible DoD affiliates as addressed in Reference (d). Consistent with applicable law, the next generation CAC will be the principal PIV credential used to facilitate physical access to facilities and installations and enable logical access to DoD networks. This guidance does not address procedures or requirements related to the use of the CAC for physical access to facilities or installations or for access to DoD networks. These areas are addressed in separate DoD guidance from USD(I) and ASD(NII).

b. In addition to the current CAC capabilities, the next generation CAC includes "contactless" technology (i.e., International Standards Organization 14443) and biometrics for personnel identification and authentication. Biometric data, such as digital fingerprints and a digital photo, are stored securely in an integrated circuit chip (ICC) providing capability for rapid authentication. Public key infrastructure (PKI) certificates stored on the card enable cardholders to "sign" documents digitally, encrypt or decrypt e-mails, authenticate to secure websites and authenticate to unclassified DoD networks. Additional technical information on the differences between the legacy CAC and next generation CAC (e.g., DoD's HSPD-12 compliant version) configurations are detailed in DMDC Guides (References (j) and (k)). All references to the CAC from this point forward are synonymous with the next generation CAC.

c. During the transition to full PIV interoperability across the Federal enterprise, there will be population categories (including non-DoD Federal Government employees affiliated with the Department) that may still require the issuance of a CAC to support their DoD assignment, benefits entitlements, or Geneva Conventions requirements. To be issued a CAC, these individuals will be required to apply for a waiver to the CAC eligibility policy included in this guidance through the Defense Human Resources

Activity (DHRA). Waivers will be reviewed and granted on a case-by-case basis until October 2009. At that time the Department expects to recognize, authenticate, and interoperate with PIV credentials issued by the individual's own agency or organization according to Reference (c).

2. GENERAL GUIDANCE. The next generation CAC will be issued at RAPIDS sites installed with CAC issuance hardware and software. This suite of equipment currently in place is being upgraded to support HSPD-12 required functionality. Migration to the next generation CAC will take place over a multi-year period. As current cards expire, the next generation CAC will be issued as part of the normal card renewal process. During this migration period, both current and next generation CACs are valid identification cards.

3. CREDENTIAL ISSUANCE. To ensure a trusted credential for increased security and interoperability within the Department of Defense and the Federal Government, the issuance of a CAC will be based on four criteria: (a) eligibility for a CAC; (b) verification of DoD affiliation from an authoritative data source; (c) completion of background vetting requirements according to Reference (c) and DoD Regulation 5200.2-R (Reference (1)); and (d) verification of a claimed identity.

a. CAC Eligibility

(1) Specific populations are automatically eligible for a CAC based on their personnel category within the Department of Defense. Examples include Uniformed Services personnel, DoD civilian employees, and specific categories of personnel assigned overseas in support of the Department. (See Section 16 of this attachment for details on the personnel categories eligible for each type of CAC.)

(2) CAC eligibility for other populations, including DoD contractors, non-DoD Federal civilians, State employees, and other non-DoD affiliates, is based on the DoD government sponsor's determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission. To be eligible for a CAC, the access requirement must meet one of the following criteria:

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

(b) The individual requires both access to a DoD facility and access to DoD networks on site or remotely.

(c) The individual requires remote access to DoD networks that use only the CAC logon for user authentication.

(3) CAC eligibility for non-U.S. persons is based on DoD Government sponsorship. Non-U.S. persons are eligible for CACs only if they meet one or more of the following:

(a) Possess legal residence status within the United States for a minimum of 3 years, a positive result from FBI fingerprint check, and an initiated National Agency Check with Written Inquiries (NACI) or equivalent as listed in this memorandum or authorized by the Deputy Under Secretary of Defense for Human Intelligence, Counterintelligence, and Security (DUSD(HC&S)).

(b) Possess a successfully adjudicated NACI or equivalent as listed in this DTM or as authorized by DUSD(HC&S).

(c) Meet (as direct/indirect DoD hire personnel) the investigative requirements for DoD employment as recognized through international agreements pursuant to Subchapter 1231, "Employment of Foreign Nationals," of DoD 1400.25-M (Reference (m)).

(d) 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 Reference (g).

b. Authoritative Data Source. According to USD(P&R) Memorandum (Reference (n)), CAC eligible personnel must be registered in the DEERS through either an authoritative personnel data feed from the appropriate Service or Agency or CVS. A number of CAC-eligible personnel categories continue to exist (including non-appropriated fund (NAF) civilians and DoD affiliates) that are not locked down through an authoritative data source. These individuals will continue to be entered into DEERS using Department of Defense (DD) Form 1172-2 as long as the remaining issuance criteria have been met.

c. Background Vetting

(1) The CAC-eligible population will not be issued a CAC without the required background vetting according to Reference (c), Reference (l), and Office of Management and Budget (OMB) Memorandum M-05-24 (Reference (o)). Initial issuance of a CAC requires, at a minimum, the completion of FBI fingerprint check with favorable results and submission of a National Agency Check with Inquiries to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. Table 1 contains an

authoritative list of background investigation for PIV that include those approved by DUSD(HC&S) as being equivalent to (or greater than) NACI.

Table 1. List of DoD Investigations

Investigation Type	JPAS Code	NACI Equiv	Description
ANACI	AN	Yes	Access National Agency Check plus Written Inquires and 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
BITN	F	Yes	Background Investigation (10 year scope)
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 and 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
NACLCLC	XX	Yes	National Agency Check, Local Agency Check and Credit Check
NACP	6	Yes	National Agency Check plus 10 Years Service
NACS	E	Yes	National Agency Check/National Agency Check plus Written Inquires and Credit Check plus Single Scope B.I. Requested
NACW	C	Yes	National Agency Check plus Written Inquires and 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 and 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

Table 1. List of DoD Investigations, Continued

Investigation Type	JPAS Code	NACI Equiv	Description
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
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
CNAC	CN	No	National Agency Check plus Credit Check
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 Check
NACFI	48	No	Non-Appropriated Fund Suitability Determination
NSI	46	No	NSI — NACI/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

(2) Currently, the Department has not established a uniform policy for adjudicating background investigations for DoD CAC PIV issuance purposes. DoD Components shall use OPM Memorandum, “Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12,” (Reference (p)) as a guide until further DoD level guidance is provided.

(3) The methods for verifying completion of the background vetting requirement within the DoD CAC issuance infrastructure are based on the personnel category of the potential CAC recipient. The mechanisms required to verify completion of background vetting activities for DoD military and civilian CAC populations are managed within the DoD human resources and personnel security communities and 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; therefore, Government sponsors are

Change 3, 09/27/2011

responsible for ensuring that the vetting requirements have been met before approving CAC issuance for all populations. Government sponsors should refer to their employer organizations and local personnel security offices, as well OPM Federal Investigations Notice 06-04 (Reference (q)), for specifics on completing the background vetting requirement. Approval of the CAC request is the Government sponsor's affirmation that the vetting requirement has been met. Contractors will submit request for investigations through their sponsoring human resources or security offices for submission to OPM. Applicants with a current NACI or DoD equivalent need not be reinvestigated.

(4) In the future, DEERS/RAPIDS workstations will be able to verify that the background vetting processes have been initiated and/or successfully completed from DoD or Federal Government authoritative data sources. Once this capability is in place, any CAC applicant that is identified within RAPIDS as not meeting the required vetting criteria will be directed to their local human resource offices, personnel security offices, or Government sponsor to initiate the vetting process or verify that the vetting has been completed.

(5) OMB is establishing guidelines for processing HSPD-12 credentials for foreign nationals. Once this guidance has been provided, the Department of Defense will provide further guidance. Until that time, foreign national personnel will have vetting verified by DoD Government sponsors according to Attachment 3, section 3.a.(3) of this DTM.

d. Identity Verification. During the CAC issuance process, all personnel will present two forms of identification in their original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB 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 (ID). The identity documents will be inspected for authenticity and scanned and stored in the DEERS according to the RAPIDS User Guide (Reference (r)) upon issuance of an ID. The photo ID requirement cannot be waived, consistent with applicable statutory requirements.

4. SEPARATION OF DUTIES. In accordance with Reference (c), DEERS/RAPIDS site security managers (SSMs) and verification officials (VOs) shall not exercise the role of the CVS TASM, TA, or the signatory sponsor on the DD Form 1172-2. Authorizing DEERS/RAPIDS SSMs or VOs to exercise the duties of a CVS TASM, TA, or sponsor would, in essence, allow a single individual to control the credential issuance process, from record creation to credential issuance.

5. CROSS SERVICING. Any RAPIDS ID card issuance facility shall, upon presentation of the required documentation and verification through DEERS, issue a CAC to an eligible recipient according to this guidance and DoDI 1000.13 (Reference (s)).

6. EXPIRATION DATE. CACs will 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 should 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 would be issued a CAC with a 3-year expiration. PKI certificates on the CACs will match the expiration date on the card with exception of Service Academy students, who are issued 4-year cards with 3-year certificates.

7. RENEWALS. A CAC holder shall be allowed to apply for a renewal starting 90 days prior to the expiration of a valid ID. The Service project office can provide exceptions to this policy. The card issuer will verify the cardholder's identity against the biometric information stored in DEERS. Consistent with applicable law, the applicant shall be required to provide two forms of identity source documents in original form:

a. The identity source documents must come from the list of acceptable documents included in Form I-9.

b. At least one document from the I-9 list shall be a valid (unexpired) State or Federal Government-issued picture ID.

8. REISSUANCE. A CAC will be reissued when:

a. 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 DEERS. Consistent with applicable law, the applicant shall be required to provide identity source documents as noted in paragraphs 7.a. and 7.b. of this attachment.

b. The CAC is reported lost or stolen. The card issuer will verify the cardholder's identity against the biometric information stored in DEERS and confirm the expiration date of the missing CAC. The individual shall be required to present documentation from the local security office or CAC sponsor confirming that the CAC has been reported lost or stolen. This documentation must be scanned and stored in DEERS. The individual reporting a lost or stolen ID shall be required to provide identity source documents as

noted in paragraphs 7.a. and 7.b. of this attachment, consistent with applicable law. The replacement CAC will have the same expiration date as the lost or stolen card.

(1) If no identity documentation is available but the picture and biometric in the DEERS database can be verified by the issuing official, a CAC can be re-issued to the individual upon the additional approval of the SSM. SSM approval may only be given for reissuance of a lost or stolen CAC.

(2) If the picture and biometric cannot be verified, the requirements for initial issuance apply, including approval from an authoritative data source.

9. MULTIPLE CARDS. There are individuals within the Department of Defense who have multiple personnel category codes with the Department (e.g., an individual that is both a reservist and a contractor). They shall be issued a separate ID card in each personnel category for which they are eligible. Multiple current CACs will not be issued or exist for an individual under a single personnel category code.

10. RETRIEVAL AND DESTRUCTION OF THE CAC. Unauthorized possession of an official identification card, like a CAC, can be prosecuted criminally under section 701 of title 18, United States Code (U.S.C.) (Reference (t)), which prohibits photographing or otherwise reproducing or possessing DoD identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both. Local commands, installations, and sponsors of contract support personnel and other eligible CAC holders shall establish procedures to ensure that the issuance and retrieval of government furnished equipment (GFE) CACs are part of the normal personnel check-in and check-out processes. These procedures will identify who will have responsibility to retrieve CACs from government personnel leaving government service and for any sponsored contract support personnel who are no longer supporting their organization and/or activity. These CACs shall be documented and treated as PII, according to Reference (h) and Reference (i), and receipted to the RAPIDS site for disposition.

a. Invalid, inaccurate, inoperative, terminated, or expired CACs shall be returned to a RAPIDS site for disposition. The CAC is the property of the U.S. Government and shall not be retained by the cardholder upon expiration, replacement, or when the DoD affiliation of the employee has been terminated.

b. Upon request, next of kin may obtain the CAC for an individual who has perished in the line of duty. All CACs provided to next of kin must be terminated, have the certificates revoked, and have a hole punched through the ICC prior to release.

11. COPYING OR DISTRIBUTION OF CARDS

a. Reference (t) prohibits photographing or otherwise reproducing or possessing DoD identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both. The credential may only be photocopied to facilitate DoD benefits and entitlements for which the card is used. When possible, the card will be electronically authenticated in lieu of photographing the card.

b. There are instances where graphical representations of CACs are necessary to facilitate the DoD mission. When used or distributed, these graphical representations must not be the same size as the CAC and must have the word "SAMPLE" written on them.

12. RESTRICTIONS. The CAC 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 CAC. Holes shall not be punched into the CAC, except as required by section 10 of this attachment. The chip or laminate shall not be removed from the CAC.

13. COLOR CODING. The CAC shall be color coded as indicated in Table 2 to reflect the status of the holder of the card.

Table 2. Card Holder Status

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. personnel under contract to the Department (other than those persons requiring a Geneva Conventions card)

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

b. Reference (c) reserves the color red to distinguish emergency first responder officials. However, policy governing the requirements for a first responder program has not been codified within the Department.

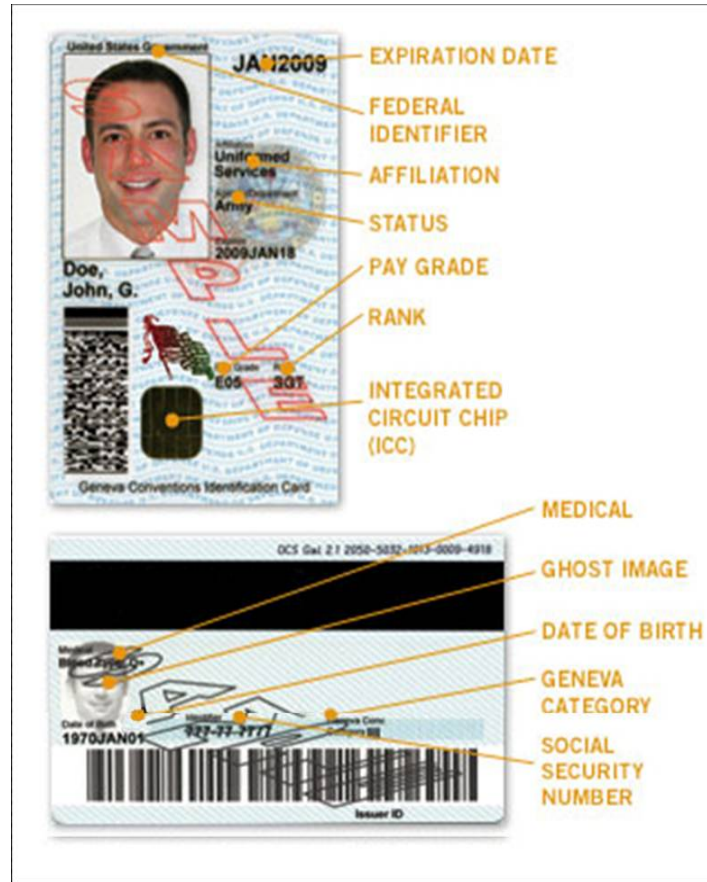
Change 3, 09/27/2011

14. PROTECTIVE SLEEVES. See Attachment 2 (Roles and Responsibilities) for DMDC and the Heads of DoD Components.

15. PUBLIC KEY INFRASTRUCTURE. Using the RAPIDS platform, the identity certificate will be issued on the CAC at the time of card issuance in compliance with the “X.509 Certificate Policy for the United States Department of Defense” (Reference (u)). E-mail signature and e-mail encryption 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 e-mail address assigned to them, they may return to a RAPIDS terminal, user maintenance portal, or post issuance portal to receive their e-mail certificate when the e-mail address has been assigned. Upon loss, destruction, or revocation of the CAC, the certificates thereon are revoked and placed on the certificate revocation list according to Reference (u). All other situations that pertain to the disposition of the certificates are handled according to Reference (u) as implemented.

16. CAC TYPES AND ELIGIBILITY. There are currently four CAC types that are used within the Department, based on cardholder eligibility. Each type will evolve into a next generation CAC type, as pictured below.

Figure 1. Armed Forces of the United States Geneva Conventions ID Card



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

(1) 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 circuit chip of the card (active duty, Reserve, National Guard). It is necessary that this chip be updated when status changes occur (e.g., mobilization, Reserve, on active duty).

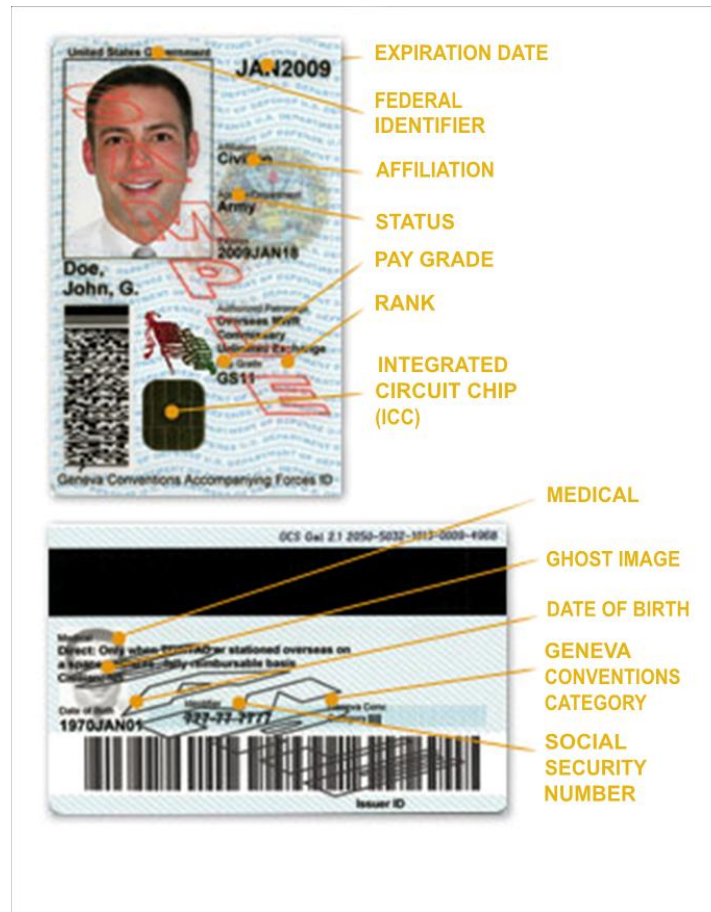
(2) The next generation CAC does not change current benefits and entitlements, or the requirement to update the DEERS when any changes to a member's family, status, or other information changes.

(3) The DD Form 2 machine-readable card will continue to be issued to those Reserve Component categories not eligible for the CAC (e.g., IRR, standby Reserve, and inactive National Guard).

(4) DD Form 1934 remains valid and will continue to be issued according to DoDI 1000.1 (Reference (v)).

(5) If a member has been mobilized and there are no communications either with the DEERS database 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 PKI certificates and will be replaced as soon as the member can reach an online RAPIDS station or communications have been restored.

Figure 2. U.S. DoD/Uniformed Services Geneva Conventions ID Card for Civilians Accompanying the Armed Forces



b. U.S. DoD/Uniformed Services Geneva Conventions ID Card for Civilians Accompanying the Armed Forces. The CAC serves as the U.S. DoD and/or Uniformed Services Geneva Conventions identification card for civilians accompanying the Armed Forces and shall be issued according to Reference (v).

(1) This card shall be the primary ID card for:

(a) Emergency-essential employees as defined in DoD Directive 1404.10 (Reference (w)).

(b) Contingency contractor employees as defined in DoD Instruction 3020.41 (Reference (x)).

(c) Civilian noncombatant personnel who have been authorized to accompany U.S. military forces in regions of conflict, combat, and contingency operations and who are liable to be captured and detained by the enemy as prisoners of war in accordance with Reference (v).

(2) The CAC replaces DD Form 489 and DD Form 2764.

(3) DD Form 1934 remains valid and will continue to be issued according to Reference (v).

(4) Additional clarification.

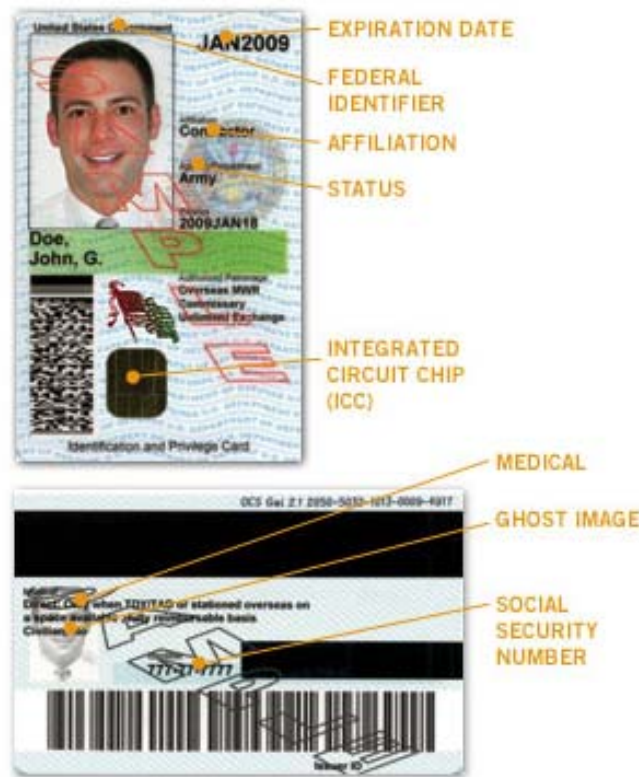
(a) Eligible individuals who are permanently assigned in foreign countries for at least 365 days (it should be noted that local nationals are in their home country, not a foreign country) will have the word "OVERSEAS" printed within the authorized patronage area of the CAC.

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

(c) During a conflict, combat, or contingency operation, civilian employees with a U.S. DoD and/or Uniformed Services Geneva Conventions ID card for civilians accompanying the Armed Forces will be granted all commissary; exchange; morale, welfare, and recreation (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.

(d) 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 according to References (w) and (x), and the Deputy Secretary of Defense Memorandum, "Policy Guidance for Provision of Medical Care for Department of Defense Civilian Employees Injured or Wounded While Forward Deployed in Support of Hostilities" (Reference (y)).

Figure 3. U.S. DoD and/or Uniformed Services ID and Privilege Card



c. U.S. DoD and/or Uniformed Services ID and Privilege Card. The CAC shall be issued according to Reference (s). This card shall be the primary ID card granting applicable benefits and privileges for civilian employees, contractors, and foreign national military, as well as other eligible personnel in the following categories:

- (1) 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.
- (2) DoD and Uniformed Services civilian employees when stationed or employed and residing in foreign countries for a period of at least 365 days.
- (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.
- (4) DoD contractors when stationed or employed and residing in foreign countries for a period of at least 365 days.

(5) DoD 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 CONUS. Within the National Capital Region (NCR), charges for outpatient care are waived. Charges for inpatient and/or outpatient care provided outside the NCR will be at the interagency rates.

(6) Civilian employees of the Army and Air Force Exchange System, Navy Exchange System, and Marine Corps Exchange System and NAF activity employees of the U.S. 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.

(7) 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.

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

(9) Foreign national military who meet the eligibility requirement of Attachment 3, section 3.a.(3) and in the following categories:

(a) Active duty officer 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 Department of Defense or a Military Department.

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

(c) Active duty officer and enlisted personnel of NATO and non-NATO countries when serving outside the United States and outside their own country under the sponsorship or invitation of the 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.

(10) The CAC replaces DD Form 2765 and DD Form 2574. Use of these forms for those eligible for the CAC is no longer authorized. The CAC also will be used to

facilitate standardized, uniform access to DoD facilities, installations, and computer systems.

Figure 4. U.S. DoD/Uniformed Services ID Card



d. U.S. DoD/Uniformed Services ID Card. This CAC shall be the primary ID card for eligible civilian employees, contractors, and foreign national affiliates that do not receive the identification and privilege CAC.

(1) DoD civilian employees are automatically eligible for this CAC, including:

(a) Individuals appointed to appropriated fund and non-appropriated fund positions (including civilian employees of the U.S. Coast Guard and NOAA).

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

(c) Senior Executive Service (SES), Competitive Service, and Excepted Service employees.

(2) The following personnel are eligible for this CAC based on the Government sponsor's determination of the type and frequency of access required to DoD facilities or networks:

Change 3, 09/27/2011

(a) Civilian employees, including:

1. Civilian employees of other Federal agencies working in support of the Department of Defense.

2. State employees working in support of the National Guard.

3. Intergovernmental Personnel Act (IPA) employees.

(b) DoD contractors.

(c) Foreign national affiliates who meet the eligibility requirements in Attachment 3, section 3.a.(3) to include:

1. 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).

2. 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 DoD facility and/or require access to DoD networks both on site or remotely (remote access must be on an exception only basis for this category). These individuals are not paid or provided benefits under any arrangement with the United States.

(3) CAC eligibility for DoD contractors, non-DoD Federal civilians, State employees, and other non-DoD affiliates is based on the government sponsor's determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission.

GLOSSARY

DEFINITIONS

Unless otherwise noted, the following terms and their definitions are for the purpose of this DTM only.

access to a DoD 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 DoD 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 (VPN), and remote administration by DoD or non-DoD personnel.

background investigations. An investigation required for determining the eligibility of an applicant for PIV credentialing.

civilian employee. DoD civilian employees, as defined in section 2105 of title 5, U.S.C. (Reference (z)), are individuals appointed to positions by designated officials. 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 SES, Competitive Service, and Excepted Service positions. In addition, the Department of Defense employs individuals paid from NAFs, as well as foreign national citizens outside the United States, its territories, and its possessions, in DoD activities overseas. The terms and conditions of host-nation citizen employment are governed by controlling treaties, agreements, and memorandums of understanding with the foreign nations.

civilian noncombatant personnel. 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 be captured and detained by the enemy as prisoners of war.

competitive service positions. See section 2102 of Reference (z).

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. This includes employees of external support, systems support, and theater support contractors.

contingency operation. See Joint Publication 1-02 (Reference (aa)).

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

excepted service positions. See section 2103 of Reference (z).

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 DTM 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.

foreign military personnel

sponsored NATO and PFP personnel in the United States. Active duty officer and enlisted personnel of NATO and PFP countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department.

sponsored non-NATO personnel in the United States. Active duty officer and enlisted personnel of non-NATO countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department.

NATO and non-NATO personnel outside the United States. Active duty officer and enlisted personnel of NATO and non-NATO countries when serving outside the United States and outside their own country under the sponsorship or invitation of the 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 NATO personnel in the United States. Active duty officer and enlisted personnel of NATO countries who, in connection with their official NATO duties, are stationed in the United States and are not under the sponsorship of the Department of Defense or a Military Department, are not eligible for a CAC, and will continue to receive a DD Form 2765.

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

foreign national positions (direct hire). See section 1581 of title 10, U.S.C. (Reference (ab)).

foreign national positions (indirect hire). See section 1581 of Reference (ab).

full-time work schedule. Full-time employment with a basic 40-hour work week.

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.

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

IPA employees. The IPA mobility program provides temporary assignment of personnel between the Federal/State/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.

National Agency Check with Written Inquiries (NACI). A personnel security investigation combining a National Agency Check and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools. All NACIs conducted for the Department of Defense shall include a credit check.

NAF employees. Federal employees within the Department of Defense who are paid from NAFs. Reference (q) explains the status of NAF employees as federal employees.

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 SES, Competitive Service, or an appointment in the Excepted Service that carries no restrictions or conditions.

seasonal employment. Annually recurring periods of work of less than 12 months each year. Seasonal employees generally are permanent employees who are placed in non-duty and/or non-pay status and recalled to duty according to pre-established conditions of employment. Seasonal employees may have full-time, part-time, or intermittent work schedules.

servicing security office. The security office assigned responsibility for providing security support to the organization responsible for CAC applicants.

SES positions. Appropriated fund positions in an agency classified above GS-15 pursuant to section 5108 or in level IV or V of Reference (z), 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 of Reference (z).

sponsor. An active duty member or civil servant who approves a CAC request.

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.