Department of Defense
INSTRUCTION

NUMBER 1000.13
January 23, 2014
Incorporating Change 1, Effective December 14, 2017

USD(P&R)

SUBJECT: Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5124.02 and DoD Instruction (DoDI) 1000.25 (References (a) and (b)), this Instruction:

a. Reissues DoD Instruction (DoDI) 1000.13 (Reference (c)) to establish policy, assign responsibilities, and provide procedures for the issuing of DoD ID cards.

b. Incorporates and cancels Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 (Reference (d)), Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and DoD Chief Information Officer DTMs 01-002 and 02-001 (References (e) and (f)), and USD(P&R) Memorandums (References (g) through (i)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), 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 DoD (hereafter referred to collectively as the "DoD Components").

b. The Commissioned Corps of the U.S. Public Health Service (USPHS), under agreement with the Department of Health and Human Services, and the National Oceanic and Atmospheric Administration (NOAA), under agreement with the Department of Commerce.

3. POLICY. It is DoD policy that:

a. A distinct DoD ID card shall be issued to uniformed service members, their dependents, and other eligible individuals and will be used as proof of identity and DoD affiliation.

b. DoD ID cards shall serve as the Geneva Convention Card for eligible personnel in accordance with DoDI 1000.01 (Reference (j)).

c. DoD ID cards shall be issued through a secure and authoritative process in accordance with Reference (b).

d. The common access card (CAC), a form of DoD ID card, shall serve as the Federal Personal Identity Verification (PIV) card for DoD implementation of Homeland Security Presidential Directive 12 (Reference (k)).

e. ID cards, in a form distinct from the CAC, shall be issued and will serve as proof of identity and DoD affiliation for eligible communities that do not require the Federal PIV card that complies with Reference (k) and Federal Information Processing Standards (FIPS) Publication 201-2 (Reference (l)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release**. This Instruction is available on the Directives Division Website at http://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 1. The changes to this issuance are administrative and update acronyms and references for accuracy.

8. EFFECTIVE DATE. This Instruction is effective January 23, 2014.

Jessica L. Wright
Acting Under Secretary of Defense for
Personnel and Readiness

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES 5

ENCLOSURE 2: RESPONSIBILITIES 7

USD(P&R) 7
ASSISTANT SECRETARY OF DEFENSE FOR MANPOWER AND RESERVE AFFAIRS (ASD(M&RA)) 7
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR MILITARY COMMUNITY AND FAMILY POLICY (DASD(MC&FP)) 7
DIRECTOR, DEFENSE HUMAN RESOURCES ACTIVITY (DHRA) 8
USD(AT&L) 8
USD(I) 8
DoD CIO 9
HEADS OF THE DoD COMPONENTS, THE DIRECTOR, USPHS, AND THE DIRECTOR, NOAA 9

ENCLOSURE 3: PROCEDURES 11

ID CARD LIFE CYCLE 11
GUIDELINES AND RESTRICTIONS 12
CAC MIGRATION TO FEDERAL PIV REQUIREMENTS 13

GLOSSARY 15

ABBREVIATIONS AND ACRONYMS 15

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008
(b) DoD Instruction 1000.25, "DoD Personnel Identity Protection (PIP) Program," March 2, 2016
(c) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 5, 1997 (hereby cancelled)
(d) Deputy Secretary of Defense Directive-Type Memorandum 08-006, "DoD Implementation of Homeland Security Presidential Directive - 12 (HSPD-12)," November 26, 2008 (hereby cancelled)
(e) Under Secretary of Defense for Personnel and Readiness and DoD Chief Information Officer Directive-Type Memorandum 01-002, "Common Access Card (CAC)" January 16, 2001 (hereby cancelled)
(f) Under Secretary of Defense for Personnel and Readiness and DoD Chief Information Officer Directive-Type Memorandum 02-001, "Common Access Card (CAC) - Changes," April 18, 2002 (hereby cancelled)
(g) Under Secretary of Defense for Personnel and Readiness Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005 (hereby cancelled)
(h) Under Secretary of Defense for Personnel and Readiness Memorandum, "Common Access Card (CAC) Eligibility for Foreign National Personnel," March 9, 2007 (hereby cancelled)
(i) Under Secretary of Defense for Personnel and Readiness Memorandum, "New Identification Cards," May 5, 1998 (hereby cancelled)
(j) DoD Instruction 1000.01, "Identity Cards Required by the Geneva Conventions," April 16, 2012, as amended
(k) Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(l) Federal Information Processing Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013
(m) DoD Instruction 8320.03, "Unique Identification (UID) Standards Supporting for DoD Net-Centric Operations," November 4, 2015
(n) Defense Federal Acquisition Regulation Supplement (DFARS), current edition1
(o) DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended
(p) Office of Personnel Management Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," July 31, 2008
(q) DoD Directive 5400.11, "DoD Privacy Program,"October 29, 2014
(r) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(s) Sections 499, 506, 509, 701, and 1001 of title 18, United States Code
(t) Appendix 501 of title 50, United States Code (also known as "The Service members Civil Relief Act")
(u) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

[1] DFARS is available at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html.

(v) National Institute of Standards and Technology Special Publication 800-76-1, "Biometric Data Specification for Personal Identity Verification," January 2007
(w) DoD Directive 8521.01E, "Department of Defense Biometrics,"-January 13, 2016

ENCLOSURE 2

RESPONSIBILITIES

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

a. Establish minimum acceptable criteria for establishment and confirmation of personal identity, establish policy for the issuance of the DoD enterprise personnel identity credentials, and approve additional systems under the Personnel Identity Protection (PIP) Program in accordance with Reference (b).

b. Act as the Principal Staff Assistant (PSA) for the Defense Enrollment Eligibility Reporting System (DEERS), the Real-Time Automated Personnel Identification System (RAPIDS), and the PIP Program in accordance with Reference (b).

c. Maintain the DEERS data system in support of the DoD in accordance with applicable law and directives.

d. Develop and field the required RAPIDS infrastructure and all elements of field support to issue ID cards including but not limited to software distribution, hardware procurement and installation, on-site and depot-level hardware maintenance, on-site and Web-based user training and central telephone center support, and telecommunications engineering and network control center assistance.

e. In coordination with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), and the DoD Chief Information Officer (DoD CIO), establish policy and oversight for CAC life-cycle compliance with Reference (l).

f. Establish procedures that will uniquely identify personnel with specific associations with the DoD and maintain the integrity of the unique personnel identifier in coordination with the DoD Components in accordance with DoDI 8320.03 (Reference (m)).

2. ASSISTANT SECRETARY OF DEFENSE FOR MANPOWER AND RESERVE AFFAIRS (ASD(M&RA)). The (ASD(M&RA)), under the authority, direction, and control of the USD(P&R), shall develop policies and establish guidance for the National Guard and Reserve Component communities that affect benefits, entitlements, identity, and ID cards.

3. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR MILITARY COMMUNITY AND FAMILY POLICY (DASD(MC&FP)). The DASD(MC&FP), under the authority, direction, and control of the USD(P&R), shall develop policy and procedures to determine eligibility for access to DoD programs for morale, welfare, and recreation; commissaries; exchanges; lodging; children and youth; DoD schools; family support; voluntary and post-

secondary education; and other military community and family benefits that affect identity and ID cards.

4. DIRECTOR, DEFENSE HUMAN RESOURCES ACTIVITY (DHRA). The Director, DHRA, under the authority, direction, and control of the USD(P&R), shall, in accordance with Reference (b):

a. Develop policies and procedures for the oversight, funding, personnel staffing, direction, and functional management of the PIP Program.

b. Coordinate with the Principal Deputy Under Secretary of Defense for Personnel and Readiness, the Assistant Secretary of Defense for Health Affairs (ASD(HA)), and the ASD(M&RA) on changes to enrollment and eligibility policy and procedures pertaining to personnel, medical, and dental issues that affect the PIP Program.

c. Develop policies and procedures to support the functional requirements of the PIP Program, DEERS, and the DEERS client applications.

d. Secure funding in support of new requirements to support the PIP Program or the enrollment and eligibility functions of DEERS and RAPIDS.

e. Approve the addition or elimination of population categories eligible for ID cards in accordance with applicable law.

f. Establish the type and form of ID card issued to eligible population categories and administer pilot programs to determine the suitable form of ID card for newly identified populations.

5. USD(AT&L). The USD(AT&L) shall:

a. Update the Defense Federal Acquisition Regulation Supplement (Reference (n)) to support requirements for CAC and Reference (k) for contracts.

b. Ensure that the requirement for contractors to return CACs at the completion or termination of each individual's support on a specific contract is included in all applicable contracts.

6. USD(I). The USD(I) shall:

a. Establish policy for the use of DoD issued ID cards for physical access purposes in accordance with DoD 5200.08-R (Reference (o)).

b. Establish policy for military, civilian, and contractor employee background investigation, submission, and adjudication across the DoD, in compliance with References (k), (l), and Office of Personnel and Management Memorandum (Reference (p)).

7. DoD CIO. The DoD CIO shall:

a. In coordination with the USD(I), USD(P&R), and USD(AT&L), establish policy and oversight for CAC life-cycle compliance with Reference (l).

b. Provide guidance regarding the use of DoD and non-DoD identification credentials on DoD information systems, including the Federal PIV cards, for authenticating to DoD network accounts and DoD private websites.

c. Ensure that the DoD Public Key Infrastructure (PKI) conforms to all applicable FIPS to the greatest extent possible.

8. HEADS OF THE DoD COMPONENTS, THE DIRECTOR, USPHS, AND THE DIRECTOR, NOAA. The Heads of the DoD Components, the Director, USPHS, and the Director, NOAA, shall:

a. Develop and implement Component-level procedures for DoD directed policies and statutory requirements to support benefits eligibility through DEERS.

b. Develop and implement Component-level ID card life-cycle procedures to comply with the provisions of this Instruction.

c. Ensure all DoD employees, uniformed service members, and all other eligible CAC applicants, including contractor employees and other affiliate CAC applicants, have met the background investigation requirements referenced in paragraph 1.c. of Enclosure 3 of this Instruction prior to approving CAC sponsorship and registration. Background investigation status must be verified and documented by the sponsor or sponsoring organization in conjunction with application for CAC issuance.

d. Establish processes and procedures as part of the normal check-in and check-out process for collection of the CAC for all categories of DoD personnel and contractor employees when there is a separation, retirement, termination, contract termination or expiration, or CAC revocation. Since CACs contain personally identifiable information (PII), CACs and the PII contained thereon, shall be safeguarded in accordance with DoDD 5400.11 (Reference (q)), and DoD 5400.11-R (Reference (r)). CACs shall be returned to any RAPIDS issuance location for proper disposal in a timely manner once surrendered by the CAC holder.

e. Provide appropriate space and staffing for all DoD ID card issuing operations, as well as reliable telecommunications to and from the Defense Information Systems Agency managed Non-Classified Internet Protocol Router Network.

f. Provide funding for CAC cardstock, printer consumables, and electromagnetically opaque sleeves to Defense Manpower Data Center (DMDC).

g. Protect cardstock and consumables in accordance with the guidelines and standards issued and maintained by DMDC.

h. In accordance with Reference (l), provide electromagnetic opaque sleeves or other comparable technologies to protect against any unauthorized contactless access to the cardholder unique identification number stored on the CAC.

i. Manage the distribution and locations of CAC personal identification number (PIN) reset workstations.

j. To the maximum extent possible, and in accordance with DoD Components' designated accrediting authority guidelines, ensure networked workstations are properly configured and available for CAC holders to use the User Maintenance Portal-Post Issuance Portal service.

k. Oversee supervision of Trusted Associate Sponsorship System trusted agents (TAs) and TA security managers and ensure the number of contractors overseen by any TA is manageable.

ENCLOSURE 3

PROCEDURES

1. ID CARD LIFE CYCLE. The DoD ID card life cycle shall be supported by an infrastructure that is predicated on a systems-based model for credentialing as described in Reference (l). Paragraphs 1.a. through 1.g. of this enclosure represent the baseline requirements for the life cycle of all DoD ID cards. The specific procedures and sequence of order for these items will vary based on the applicant's employment status or affiliation with the DoD and the type of ID card issued. Detailed procedures of the ID card life cycle for each category of applicant and type of ID card shall be provided by the responsible agency.

a. Sponsorship and Eligibility. 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 must be sponsored by a DoD government official or employee.

b. Registration and Enrollment. Sponsorship and enrollment information on the ID card applicant shall be registered in DEERS prior to card issuance.

c. Background Investigation. 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. Sponsored CAC applicants shall not be issued a CAC without a favorably adjudicated background investigation stipulated in Reference (l). Applicants that have been denied a CAC based on an unfavorable adjudication of the background investigation may submit an appeal in accordance with References (l) and (p).

d. Identity and Eligibility Verification. Identity and eligibility verification shall be completed at a RAPIDS workstation. Verifying officials shall inspect identity and eligibility documentation and RAPIDS shall authenticate individuals to ensure that ID cards are provided only to those sponsored and with a current affiliation with the DoD. RAPIDS shall also capture uniquely identifying characteristics that bind an individual to the information maintained on that individual in DEERS and to the ID card issued by RAPIDS. These characteristics may include, but are not limited to, digital photographs and fingerprints.

e. Issuance. 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.

f. Use and Maintenance. 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.

g. Retrieval and Revocation. 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 an ID card shall be revoked within the DEERS and RAPIDS infrastructure and the PKI certificates on the CAC shall be revoked.

2. GUIDELINES AND RESTRICTIONS. The guidelines and restrictions of this section apply to all forms of DoD ID cards.

a. Any person willfully altering, damaging, lending, counterfeiting, or using these cards in any unauthorized manner is subject to fine or imprisonment or both, as prescribed in sections 499, 506, 509, 701, and 1001 of title 18, United States Code (U.S.C.) (Reference (s)). Section 701 of Reference (s) prohibits photographing or otherwise reproducing or possessing DoD ID cards in an unauthorized manner, under penalty of fine or imprisonment or both. Unauthorized or fraudulent use of ID cards would exist if bearers used the card to obtain benefits and privileges to which they are not entitled. Examples of authorized photocopying include photocopying of DoD ID cards to facilitate medical care processing, check cashing, voting, tax matters, compliance with appendix 501 of title 50, U.S.C. (also known as "The Service member's Civil Relief Act") (Reference (t)), or administering other military-related benefits to eligible beneficiaries. When possible, the ID card will be electronically authenticated in lieu of photographing the card.

b. International agreements (including status-of-forces agreements) and host-nation law may limit and/or define the types of support available to personnel in overseas areas. Although an ID card may be used to verify eligibility in the United States for access to, for example, commissary or exchange facilities, the use of such facilities overseas may be limited to persons who are stationed or performing temporary duty in a foreign country under official orders in support of a mutual defense mission with the host nation. ID cards shall be issued only for the purposes identified in and in accordance with this Instruction, and the Heads of the DoD Components shall use other means, such as ration cards, to implement provisions in international agreements or to prevent violations of applicable host-nation law. ID cards shall not be issued for the sole purpose of implementing provisions of international agreements or restrictions based on applicable host-nation law.

c. All ID cards are property of the U.S. Government and shall be returned upon separation, resignation, firing, termination of contract or affiliation with the DoD, or upon any other event in which the individual no longer requires the use of such ID card.

d. To prevent any unauthorized use, ID cards that are expired, invalidated, stolen, lost, or otherwise suspected of potential or actual unauthorized use shall be revoked in DEERS along with the PKI certificates on the CACs immediately revoked.

e. There are instances where graphical representations of ID cards are necessary to facilitate the DoD mission. When used and distributed, the replicas must not be the same size as the ID card, must have the word "SAMPLE" written on them, and shall not contain an individual's PII. All SAMPLE ID cards must be maintained in a controlled environment and shall not serve as a valid ID.

f. Individuals within the DoD who have multiple personnel category codes (e.g., an individual who is both a reservist and a contractor) shall be issued a separate ID card in each personnel category for which they are eligible. Multiple current ID cards of the same form (e.g., CAC) shall not be issued or exist for an individual under a single personnel category code.

g. ID cards shall not be amended, modified, or overprinted by any means. No stickers or other adhesive materials are to be placed on either side of an ID card. Holes shall not be punched into ID cards, except when a CAC has been requested by the next of kin for an individual who has perished in the line of duty. A CAC provided to next of kin shall have the status of the card revoked in DEERS, have the certificates revoked, and have a hole punched through the integrated circuit chip before it is released to the next of kin.

h. An ID card shall be in the personal custody of the individual to whom it was issued at all times. If required by military authority, it shall be surrendered for ID or investigation.

3. CAC MIGRATION TO FEDERAL PIV REQUIREMENTS. The DoD is migrating the CAC to meet the Federal requirements for credentialing contained within References (k) and (l). Migration will take place over multiple years as the card issuance hardware, software, and supporting systems and processes are upgraded. Successful migration 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). The organizations listed in this section will support the migration in conjunction with the responsibilities listed in Enclosure 2:

a. The Director, DMDC shall:

(1) Procure and distribute CAC consumables, including card stock, electromagnetically opaque sleeves, and printer supplies, commensurate with funding received from the DoD Components.

(2) In coordination with the Office of the Under Secretary of Defense for Policy, establish an electronic process for securing CAC eligibility information on foreign government military, employee, or contract support personnel whose visit status and background investigation has been confirmed, documented, and processed in accordance with DoDD 5230.20 (Reference (u)).

(3) In accordance with Reference (l), electronically capture and store source documents in the identity-proofing process at the accession points for eligible ID card holders.

(4) 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 Reference (l).

(5) Establish and implement procedures for capturing biometrics required to support CAC issuance, which includes fingerprints and facial images specified in Reference (l) and National Institute of Standards and Technology Special Publication 800-76-1 (Reference (v)).

(6) 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.

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

b. The Executive Manager for DoD Biometrics, as appointed by the Secretary of the Army as DoD Executive Agent for DoD Biometrics in accordance with DoDD 8521.01E (Reference (w)), shall:

(1) Establish biometric standards for collection, storage, and subsequent transmittal of biometric information in accordance with Reference (w).

(2) 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 References (r) and (v).

c. The Identity Protection and Management Senior Coordinating Group shall:

(1) Monitor the CAC and identity management related activities outlined within this Instruction in accordance with Reference (b).

(2) Maintain a configuration management process for the CAC and its related components to monitor DoD compliance with Reference (l).

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ASD(HA)	Assistant Secretary of Defense for Health Affairs
ASD(M&RA)	Assistant Secretary of Defense for Manpower and Reserve Affairs
CAC	common access card
DEERS	Defense Enrollment Eligibility Reporting System
DHRA	Defense Human Resources Activity
DMDC	Defense Manpower Data Center
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DTM	Directive-Type Memorandum
DASD(MC&FP)	Deputy Assistant Secretary of Defense for Military Community and Family Policy
FIPS	Federal Information Processing Standards
ID	identification
NOAA	National Oceanic and Atmospheric Administration
PII	personally identifiable information
PIN	personal identification number
PIP	Personnel Identity Protection
PIV	Personal Identity Verification
PKI	public key infrastructure
PSA	Principal Staff Assistant
RAPIDS	Real-Time Automated Personnel Identification System
TA	trusted agent
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(P&R)	Under Secretary of Defense for Personnel & Readiness
USD(I)	Under Secretary of Defense for Intelligence
USPHS	U.S. Public Health Service