OFFICE OF THE SECRETARY OF DEFENSE

1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JAN 16 2001

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Common Access Card (CAC)

In accordance with the Deputy Secretary of Defense memorandum of November 10, 1999, subject: "Smart Card Adoption and Implementation," the Department is implementing smart card technology through a common access card (CAC) and has developed four versions as described below. The CAC will be the standard identification card, the principal card used to enable physical access to buildings, installations, and controlled spaces, and will be used to enable Information Technology systems and applications that access the Department's computer networks. The CAC shall be issued and maintained using the infrastructure provided by the Defense Enrollment Eligibility Reporting System (DEERS) and the Real-time Automated Personnel Identification System (RAPIDS), as upgraded, starting in October 2000.

The "Armed Forces of the United States Geneva Conventions Identification Card" will be issued to active duty and members of the Selected Reserve of the Armed Forces. This version of the CAC will be modified (from Armed Forces) to state "Uniformed Services" for members of the National Oceanic and Atmospheric Administration and the U.S. Public Health Service. The "United States DoD/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces" will be issued to all Emergency-Essential employees, contingency contractor employees, and civilian noncombatant personnel (including both appropriated fund and nonappropriated fund employees) who are deployed in conjunction with military operations overseas. The "United States DoD/Uniformed Services Identification and Privilege Card" will be issued to sponsors eligible for a CAC, other than current or retired members of the Uniformed Services, who are eligible for Uniformed Services benefits and

FEDERAL RECYCLING PROGRAM PRINTED ON RECYCLED PAPER

privileges. The "United States DoD/Uniformed Services Identification Card" will be issued to DoD civilian employees (including both appropriated fund and nonappropriated fund employees) and eligible contractor employees. The identification cards currently issued in accordance with DoDI 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," shall remain valid until replaced with the CAC for the eligible recipients identified herein. Retirees and family members are not eligible for the CAC at this time.

This memorandum applies to the Office of the Secretary of Defense (OSD); the Military Departments; the Chairman of the Joint Chiefs of Staff; the Combatant Commands; the Inspector General of the Department of Defense (DoD); the Defense Agencies and Offices (see Definitions); and the DoD Field Activities (hereafter referred to collectively as the "DoD Components").

To facilitate use of these cards immediately, we are providing policies via this memorandum and its attachments. Responsibilities, general guidance, access control and public key infrastructure (PKI) policies relating to the CAC, images of the cards, issuing guidance for the cards, definitions, the DD Form 1172-2, "Application for Department of Defense Common Access Card – DEERS Enrollment," and instructions for completion of the form are attached. The CAC policies will be incorporated within applicable DoD issuances within 180 days. Components shall implement CAC policy consistent with their labor relations obligations.

This policy is effective immediately. The point of contact for this policy memorandum is Ms. Sheila Ford, 703 696-0404.

Bernard Rostker
Under Secretary of Defense
(Personnel and Readiness)

Arthur L. Money
DoD Chief Information Officer

Attachments:
As stated

cc:
Commandant, United States Coast Guard
Director, NOAA Corps
Director, United States Public Health Service

RESPONSIBILITIES

The Department's Chief Information Officer (DoD CIO) shall establish overall policy and oversight, and coordinate the physical design of the CAC with the Under Secretary of Defense (Personnel and Readiness) (USD(P&R)).

The USD(P&R) shall coordinate the physical design of the CAC with the DoD CIO, and 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. The Defense Manpower Data Center (DMDC), under the USD(P&R), will procure and distribute consumables, including card stock and printing supplies, commensurate with funding received from the DoD Components.

Principal Staff Assistants (PSAs) shall define joint applications requirements for the CAC in their functional area of responsibility.

The National Security Agency (NSA) has been assigned responsibility for the management of the DoD Public Key Infrastructure Program Management Office (PKI PMO) by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and DoD CIO. As such, NSA will provide system security assessments in support of the DoD PKI PMO to include the DEERS/RAPIDS infrastructure used to issue CACs (which will function as PKI tokens). The PKI PMO shall also determine PKI token security requirements and provide these to the DMDC Access Card Office.

The Heads of the DoD Components shall comply with this policy and take actions necessary to implement the use of a standard DoD smart card as specified in the Deputy Secretary of Defense memorandum of November 10, 1999, subject: "Smart Card Adoption and Implementation," and other guidance stated herein. The Heads of the DoD Components shall furnish appropriate space and staffing for card issuing operations, as well as reliable telecommunications to and from the Defense Information Systems Agency managed Non-secure Internet Protocol Network. DoD Components shall provide funding for the cardstock and printer consumables to the Access Card Office (ACO) in accordance with a Memorandum of Agreement that shall be developed by March 15, 2001, in accordance with the FY 02 Program Decision Memorandum Item Number 10 guidance. DoD Components shall also procure and fund all required smart card readers. Components shall determine Component-specific application requirements, fund, and manage those applications.

The Electronic Business Board of Directors (EB BoD) shall oversee the operation of the Smart Card Senior Coordinating Group (SCSCG). The EB BoD shall assure the integration of cross-functional requirements and approve summary-level chip storage allocations as recommended by the SCSCG and as identified for Component-specific use of the CAC. The EB BoD will include representatives (General/Flag/SES minimum) from appropriate PSAs within

the Office of the Secretary of Defense (OSD), the Joint Staff, Military Services, and appropriate Defense Agencies, and shall oversee the operation of the SCSCG.

The SCSCG, in accordance with its charter, shall develop and implement Department-wide interoperability standards for use of smart card technology and plan to exploit smart card technology as a means for enhancing deployment processing, personnel readiness, PERSTEMPO tracking, and improving business processes. The SCSCG shall accomplish these tasks by integrating smart card requirements as received from and in coordination with the DoD Components and the DoD PKI PMO, and making recommendations to include Joint Technical Architectural impacts to the DoD CIO through the EB BoD.

The ACO, in accordance with its charter, shall plan, program, acquire, field, and integrate the DoD CAC; provide operational, technical, program, policy support, and associated information management to the DoD Components on smart card matters; and provide executive secretary support to the SCSCG.

GENERAL GUIDANCE
COMMON ACCESS CARD

The CAC will be issued at Real-time Automated Personnel Identification System (RAPIDS) sites installed with CAC hardware and software. This suite of equipment began fielding worldwide early in FY 2001. The CAC is only available as generated by the RAPIDS. The CAC will be issued to eligible recipients by October 2002. Prior to October 2002, it will replace the eligible recipient's current identification card whenever that card expires, is lost or stolen, or upon direction of the local command.

The initial version of the CAC will not accommodate all of the requirements within the Department. For example, support for classified requirements will need to be accommodated through other means. Department-wide financial applications may be possible, and are being investigated, but are not supported by the CAC at this time. The CAC will replace identification cards and designated access passes. As technology evolves, the CAC will support additional requirements addressing other functional applications. Priority will be afforded to functional requirements that support the warfighting CINCs (i.e., deployment processing, personnel readiness, PERSTEMPO tracking).

CROSS SERVICING: Any authorized Uniformed Service personnel office or CAC card-issuing facility with on-line access to the Defense Enrollment Eligibility Reporting System (DEERS) shall, on presentation of the required documentation or verification through the DEERS, verify and issue an identification card or CAC to an eligible recipient in accordance with DoDI 1000.13 and this memorandum.

EXPIRATION DATES: CACs will be issued for a period of three years, or the individual's term of service, employment, or association with the DoD, whichever is earlier.

REISSUANCE: A CAC will be replaced when lost or stolen, when printed information requires changes, or when any of the media (to include printed data, magnetic stripe, either of the bar codes, or the chip) becomes illegible or inoperable.

MULTIPLE CARDS: Initially, individuals shall be issued a separate CAC or identification card (when status is in category not eligible for a CAC) in each category for which they qualify. Each CAC will have a PKI identity certificate. In instances where an individual has been issued more than one CAC, e.g., a Reservist who is also a DoD contractor employee, only the CAC that most accurately depicts the capacity in which the individual will operate with respect to the facility, will be activated for access to that facility.

There are individuals within the DoD community who have multiple affiliations with the Department. Although the issue of multiple affiliations has not been resolved for the initial implementation of the CAC, a resolution toward the goal of one CAC, regardless of the number of affiliations, is being addressed.

RETRIEVAL AND DESTRUCTION OF THE CAC: Invalid, inaccurate, inoperative, or expired CACs shall be returned to a RAPIDS site for disposition. Once retrieved and evaluated, these CACs shall either be in a totally locked state or all private keys must be erased.

CURRENT SMART CARDS: Those DoD Components currently using smart cards and smart card applications related to personnel are directed to migrate those card applications to the CAC as soon as practicable, but no later than September 30, 2003. Acquisition and logistics processes that use smart cards for materiel management, to include Impact cards and other credit cards issued by commercial contractors for government use, are unaffected by this policy. Unless otherwise authorized by the Smart Card Senior Coordinating Group, no other DoD-wide smart card use is authorized.

PROHIBITION ON COPYING OR DISTRIBUTING SAMPLE CARDS: Title 18, United States Code, section 701 prohibits photographing or otherwise reproducing or possessing departmental identification cards in an unauthorized manner, under penalty of fine or imprisonment or both. Consequently, for purposes related to communication with user communities regarding the new cards within the Department, the CAC shall not be posted or shown on web sites, or shown actual size, it will always be shown with "sample" on it, and the likenesses shown within this document will be used to the maximum extent possible.

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.

COLOR CODING: The CAC shall be color coded as indicated below to reflect the status of the holder of the card as follows:

White	U.S. citizen civilian employees, U.S. citizen military personnel, Non-U.S. citizens serving in the U.S. Armed Forces who have been lawfully admitted to the United States for permanent residence, and U.S. citizen employees and foreign national employees of DoD contractors who have been identified and approved as emergency personnel for the purpose of deploying with U.S. forces overseas and who are subject to capture.
Red	Foreign national personnel, including DoD contractor employees (other than those foreign nationals issued a white color coded CAC as indicated above).
Green	U.S. citizen personnel of DoD contractors (other than those issued a white color coded CAC as indicated above).

ACCESS

The CAC shall be used to control access to DoD facilities, installations, and controlled spaces. This does not require DoD Components to immediately dismantle current access systems. Moreover, this policy does not preclude the continued use of supplemental badging systems that are considered necessary to provide an additional level of security not presently afforded by the CAC. However, DoD activities are to plan for migration to the CAC for general access control using any of the CACs present or future access control capabilities.

U.S. citizen civilian personnel visiting a DoD facility, possessing a CAC, may be provided unescorted access in accordance with policy and procedures established by the security office responsible for the facility.

U.S. citizen and foreign national personnel visiting a DoD facility under circumstances other than those described above shall be escorted at all times while within the DoD facility.

In instances where an individual has been issued more than one CAC, e.g., a Reservist who is also a DoD contractor employee, only the CAC that most accurately depicts the capacity in which the individual will operate with respect to the facility, will be activated for access to that facility.

In accordance with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) memorandum of January 4, 1996, subject: "Uniformed Badge System for the Department of Defense," the magnetic stripe on the CAC is to comply with the Security Equipment Integration Working Group Specification 012 for the ordering of magnetic stripe information for badging and access control systems.

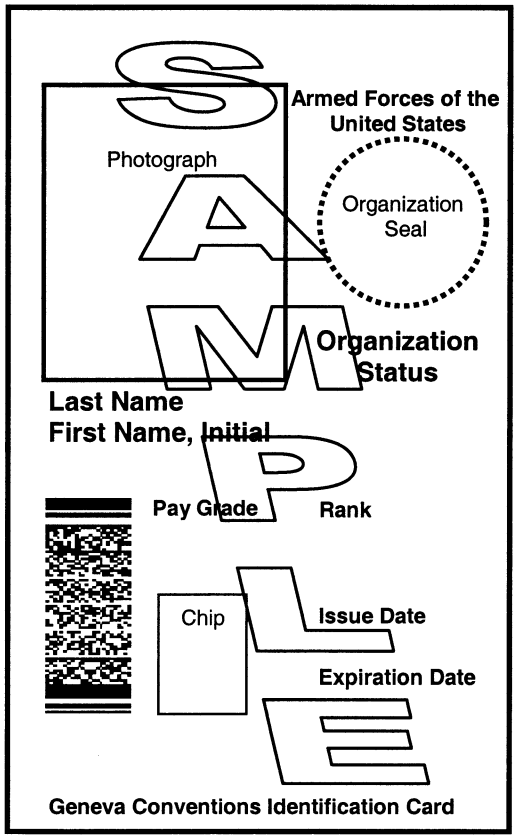
PUBLIC KEY INFRASTRUCTURE (PKI)

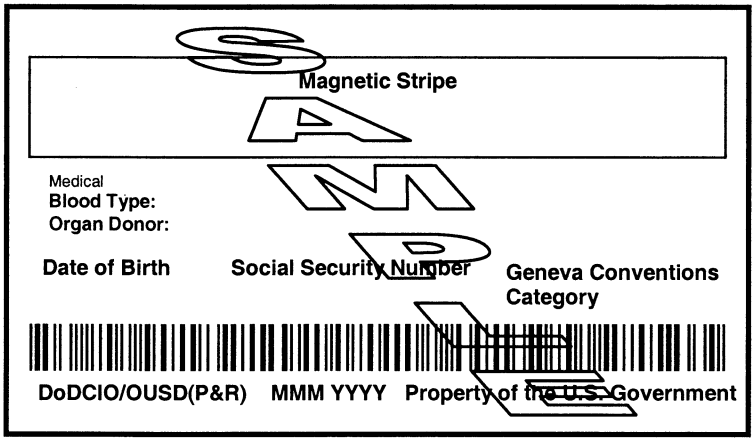
As the Department strives to achieve knowledge superiority and assure critical information to the warfighter, it recognizes the need for robust information assurance (IA) capabilities to protect the confidentiality, integrity, and authenticity of this information. To this end, the DoD is implementing a PKI -- a key and certificate management infrastructure designed to support confidentiality, integrity, availability, authentication, non-repudiation, and access control in computer networks. On May 6, 1999, the Deputy Secretary of Defense issued a memorandum (modified on August 12, 2000) that encouraged widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. The strategy to achieve the target DoD PKI is intrinsically linked to the overall DoD strategy for achieving IA. On November 10, 1999, the Deputy Secretary of Defense directed that the CAC be used as the DoD's primary platform for the PKI authentication token. A report to Congress, "Consideration of Smart Cards as the DoD PKI Authentication Device Carrier" dated January 10, 2000, was submitted in compliance with section 374 of the fiscal year

(FY) 2000 Defense Authorization Act (Public Law 106-65), requiring the evaluation of the option of using the smart card as the DoD's authentication token. The report concludes the smart card is the most feasible, cost-effective technology for the authentication mechanism to support the DoD PKI and to protect its critical information.

Using the RAPIDS platform, identity certificates 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, Version 5.0, dated December 13, 1999. E-mail signature and e-mail encryption certificates may be loaded onto the CAC either upon issuance or at some other time. If a person receiving a CAC has an e-mail address, they may have e-mail certificates loaded at the time the CAC is issued. If the person receiving a CAC does not have an e-mail address assigned, they may return to a RAPIDS terminal to receive their e-mail certificates when the E-mail address has been assigned. Upon loss, destruction, or revocation of the CAC, the certificates thereon will be revoked and placed on the Certificate Revocation List (CRL) in accordance with X.509 Certificate Policy. All other situations that pertain to the disposition of the certificates will also be handled in accordance with the X.509 Certificate Policy, as implemented.

Armed Forces of the United States
Geneva Conventions Identification Card





Armed Forces of the United States
Geneva Conventions Identification Card

The Armed Forces of the United States Geneva Conventions Identification Card is the primary identification, and physical and logical access card for active duty Uniformed Services' members, Selected Reserve members, and members of the National Guard and shall be used for access to DoD facilities and systems access, serve as the member's Geneva Conventions Identification Card, and identify the member's eligibility for benefits and privileges administered by the Uniformed Services. This version of the CAC will be modified (from Armed Forces) to state "Uniformed Services" for members of the National Oceanic and Atmospheric Administration and the U.S. Public Health Service.

In the Status area of the card, the card will show:

ACTIVE DUTY for members on Active Duty, and
RESERVE for members of the Selected Reserve not on active duty or full-time National Guard duty in excess of 30 days.

When a Reserve member is on Active duty or a National Guard member is on full-time duty in excess of 30 days a new CAC will be issued with the designation "ACTIVE" in Status area of the CAC. Ultimately, the goal is for a single CAC for all Armed Forces personnel in which the member's status is maintained electronically.

The CAC does not change current benefits, entitlements, or requirements to update the Defense Enrollment Eligibility Reporting System (DEERS). At this time, Commissary Cards still are required for members of the Reserve Components.

The expiration date on the CAC will be the earliest of three years, the date of expiration of term of active service, expected date of graduation, or expiration of enlistment contract. Current DD Forms 2 remain valid until their expiration date or replacement by a CAC.

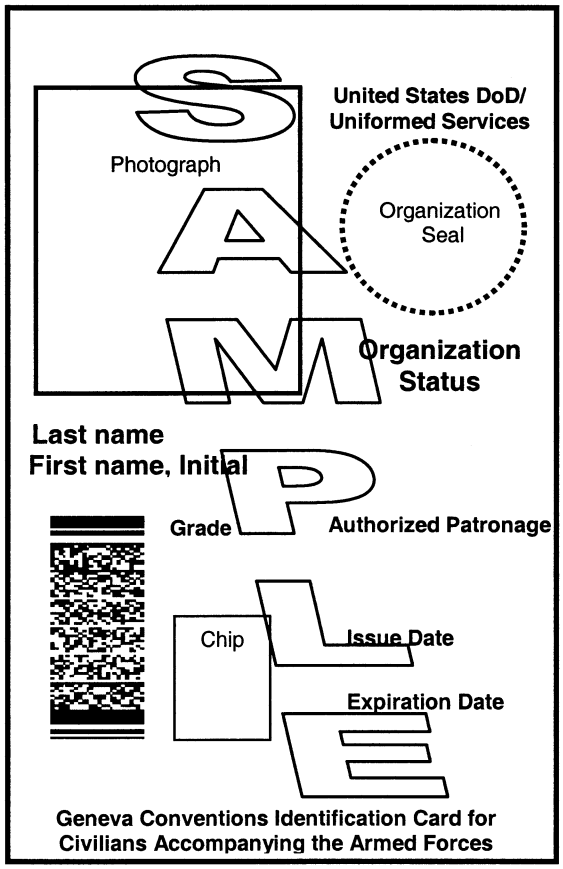
The CAC replaces the DD Form 2, U.S. Armed Forces Identification Card (Active), manually-prepared card; the DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Active), machine-readable card; the DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Reserve), manually prepared card; and the DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Reserve), machine-readable card for those eligible for the CAC. The cards listed above, for those eligible for the CAC, will expire upon fielding of the CAC software and complete implementation of the CAC. The CAC also will be used to facilitate standardized, uniform access to DoD facilities, installations, and computer systems.

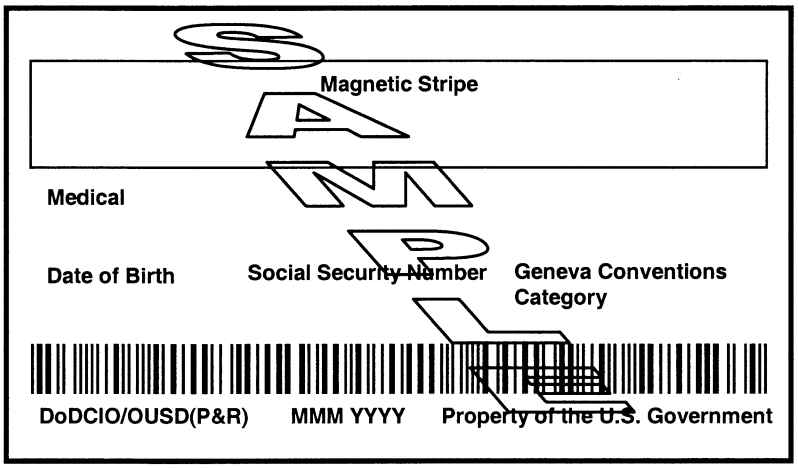
The DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Reserve), machine-readable card will continue to be issued to those Reserve Component categories not eligible for the CAC, i.e., Individual Ready Reserve, Standby Reserve, and Inactive National Guard.

The DD Form 1934, Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces, remains valid and will continue to be issued in accordance with DoDI 1000.1, Identity Cards Required by the Geneva Conventions.

When there are no communications either with the DEERS database or the DoD certificate authority, a temporary card can be issued with an abbreviated expiration date for a minimum of 10 and maximum of 280 days. The temporary card will not have a chip, nor will it have PKI certificates. The temporary card will appear the same as the Armed Forces of the United States Geneva Conventions Identification Card with a white space where the chip is normally.

United States DoD/Uniformed Services
Geneva Conventions Identification Card
for Civilians Accompanying the Armed Forces





United States DoD/Uniformed Services
Geneva Conventions Identification Card
for Civilians Accompanying the Armed Forces

The United States DoD/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces shall be issued in accordance with DoD Instruction 1000.1, "Identity Cards Required by the Geneva Conventions," and shall be the primary identification and physical and logical access card for the following individuals:

1. Emergency-Essential employees as defined in DoD Directive 1404.10.

2. Contingency contractor employee (see Definitions).

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

EXCEPTION: Since the Defense Eligibility Enrollment Reporting System (DEERS) is the platform from which the CAC is generated, and personnel information on employees of the Intelligence Community (e.g., National Security Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, and National Reconnaissance Office) is not maintained in DEERS, civilian employees of the Intelligence Community will not be issued a CAC.

In the Status area of the card, the card will show:

CIVILIAN for civilian employees,
CONTRACTOR for contractor employees, and
AFFILIATE for civilians who are neither civilian nor contractor employees

The expiration date on this card will be the earliest of three years or expected termination of the recipient's association with DoD.

The CAC replaces the DD Form 489, Geneva Conventions Identify Card for Persons Who Accompany the Armed Forces, and the DD Form 2764, United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card for those eligible for the CAC. The cards listed above, for those eligible for the CAC, will expire upon fielding of the CAC software and complete implementation of the CAC. The CAC also will be used to facilitate standardized, uniform access to DoD facilities, installations, and computer systems.

The DD Form 1934, Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces, remains valid and will continue to be issued in accordance with DoDI 1000.1, Identity Cards Required by the Geneva Conventions.

When there are no communications either with the DEERS database or the DoD certificate authority, a temporary card can be issued with an abbreviated expiration date for a minimum of 10 and maximum of 280 days. The temporary card will not have a chip, nor will it have PKI certificates. The temporary card will appear the same as the United States DoD/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces with a white space where the chip is normally.

NOTES:

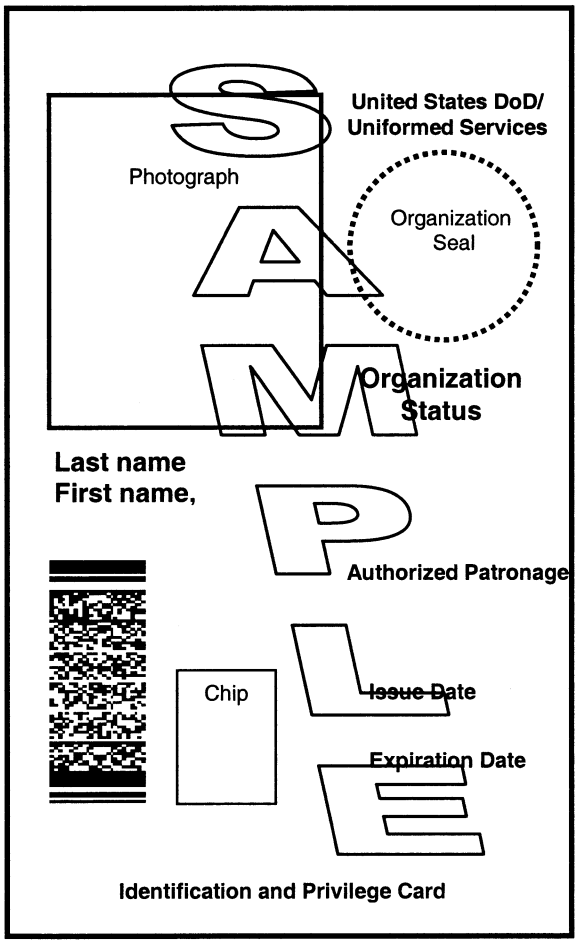
N1. The Authorized Patronage block for eligible individuals who are permanently assigned in foreign countries (it should be noted that local nationals are in their home country, not a foreign country) will have the word "OVERSEAS" printed within the block of the CAC.

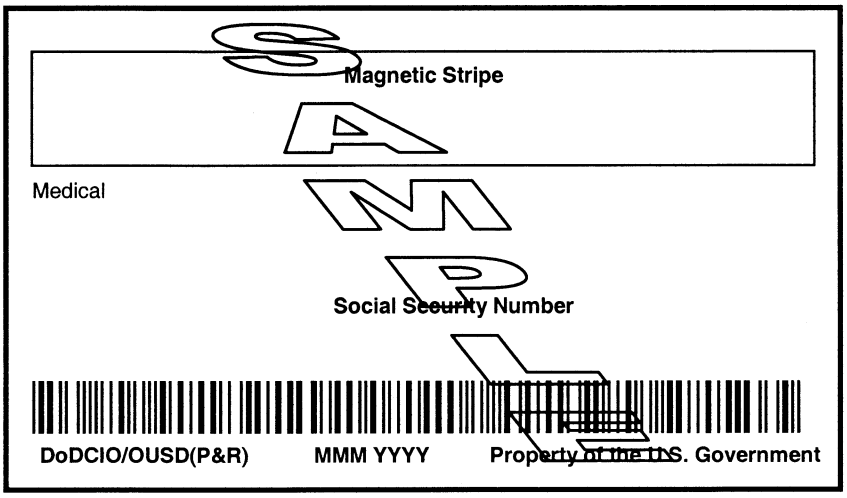
N2. The Authorized Patronage block for eligible individuals permanently assigned within CONUS will be blank. Travel orders authorize access for these individuals while en route to the deployment site.

N3. During a conflict, combat, or contingency operation, civilian employees with a United States DoD/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces will be granted all commissary, exchange, MWR, and medical privileges available at the site of the deployment, regardless of the statements on the identification 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.

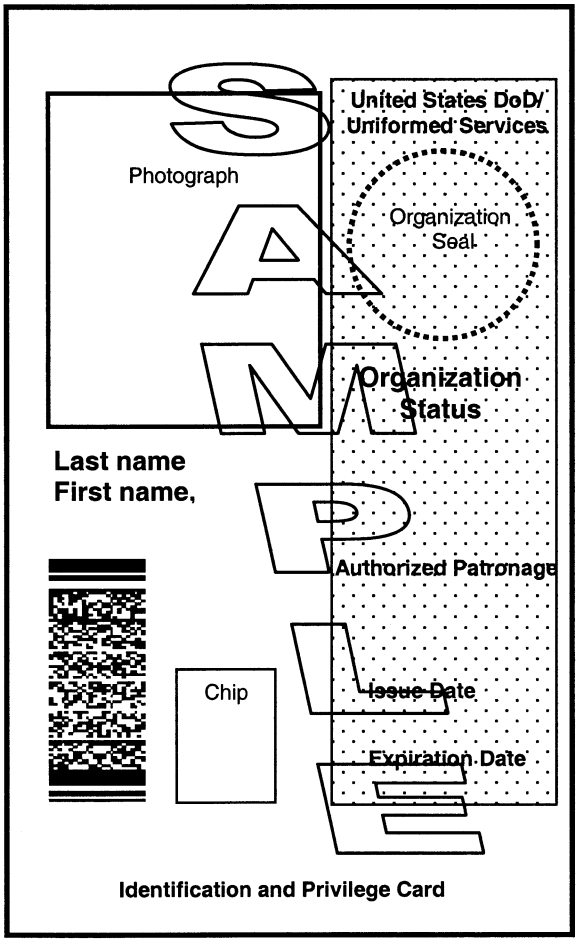
N4. The medical block on this card will contain a statement, "When TAD/TDY or stationed overseas on a space-available fully reimbursable basis." However, civilian employees and contractual services employees providing support when forward deployed during a conflict, combat, or contingency operation are treated in accordance with the ASD(HA) memorandum of January 8, 1997, subject: "Medical Care Costs for Civilian Employees Deployed in Support of Contingency Operations." This policy states that it is not considered practicable or cost-effective to seek reimbursement from civilian or contractor employees or third party payers for medical services. However, where a civilian or contractor employee is evacuated for medical reasons from the contingency area of operations to a medical treatment facility (MTF) funded by the Defense Health Program (DHP), normal reimbursement policies would apply for services rendered by that facility.

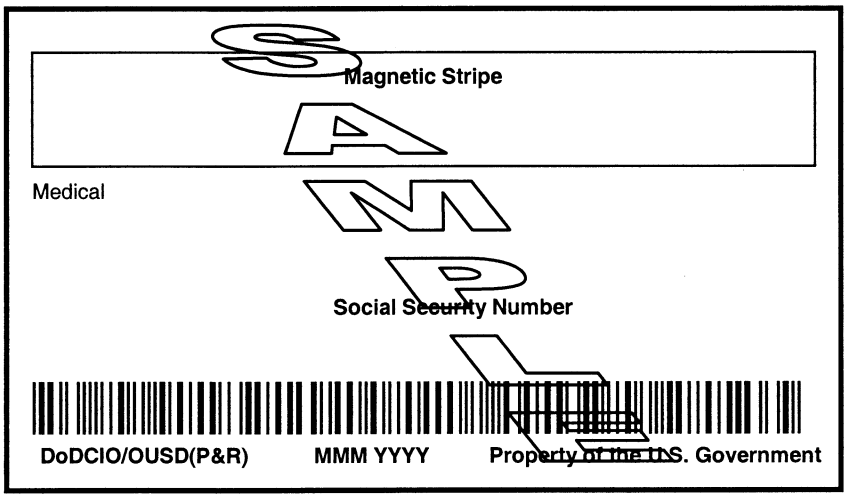
United States DoD/Uniformed Services Identification and Privilege Card





United States DoD/Uniformed Services
Identification and Privilege Card
With Color Band for Designated Contractor Employees
And Foreign Nationals





United States DoD/Uniformed Services Identification and Privilege Card

The United States DoD/Uniformed Services Identification and Privilege Card shall be issued in accordance with DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," and DoD Instruction 1000.23, "Department of Defense Civilian Identification (ID) Card" and shall be the primary identification (granting applicable benefits and privileges), and physical and logical access card for civilian employees in the following categories:

Civilian employees of the DoD and the Uniformed Services, when required to reside in a household on a military installation within the Contiguous United States (CONUS), Hawaii, Alaska, Puerto Rico, and Guam.

Civilian employees of the DoD, the Uniformed Services, and civilian personnel under private contract to the DoD or a Uniformed Service, when stationed or employed and residing in foreign countries for a period of at least 365 days.

DoD Presidential Appointees who have been appointed with the advice and consent of the Senate. (See note 1.)

Civilian employees of the Army and Air Force Exchange System, Navy Exchange System, and Marine Corps Exchange System. (See note 2.)

Foreign Military Personnel—see definitions.

EXCEPTION: Since the Defense Eligibility Enrollment Reporting System (DEERS) is the platform from which the CAC is generated, and personnel information on employees of the Intelligence Community (e.g., National Security Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, and National Reconnaissance Office) is not maintained in DEERS, civilian employees of the Intelligence Community will not be issued a CAC.

In the Status area of the card, the card will show:

EXECUTIVE for Executive Level employees
CIVILIAN for civilian employees, and
CONTRACTOR for contractor employees
FOREIGN MILITARY for authorized foreign military personnel

The expiration date on this card will be the earliest of three years or expected termination of the recipient's employment or association with the Department.

The CAC replaces the DD Form 2765, DoD/Uniformed Services Identification and Privilege Card and DD Form 2574, Exchange Service Identification and Privilege Card, for those eligible for the CAC. The DD Form 2765, for those eligible for the CAC, will expire upon fielding of the CAC software and complete implementation of the CAC. The CAC also will be

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

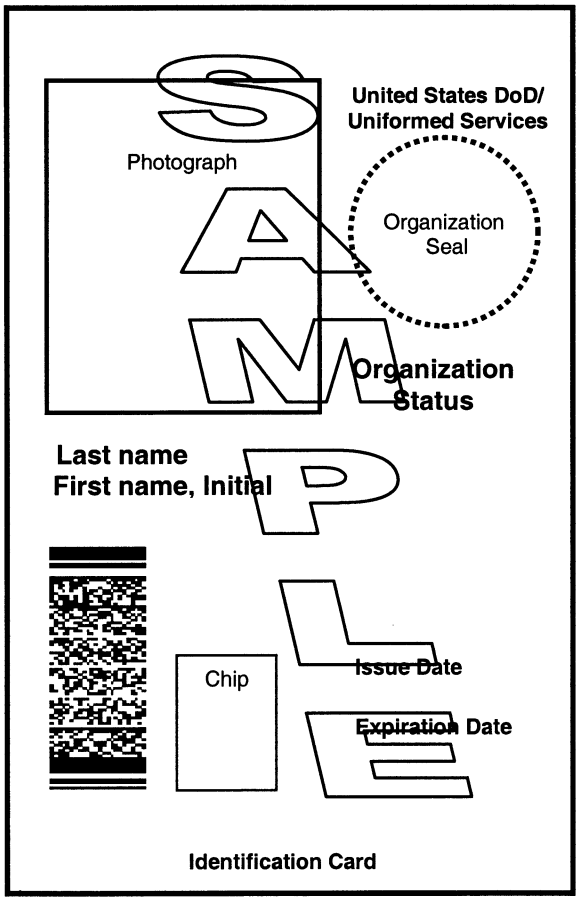
When there are no communications either with the DEERS database or the DoD certificate authority, a temporary card can be issued with an abbreviated expiration date for a minimum of 10 and maximum of 280 days. The temporary card will not have a chip, nor will it have PKI certificates. The temporary card will appear the same as the United States DoD/Uniformed Services Identification and Privilege Card with a white space where the chip is normally.

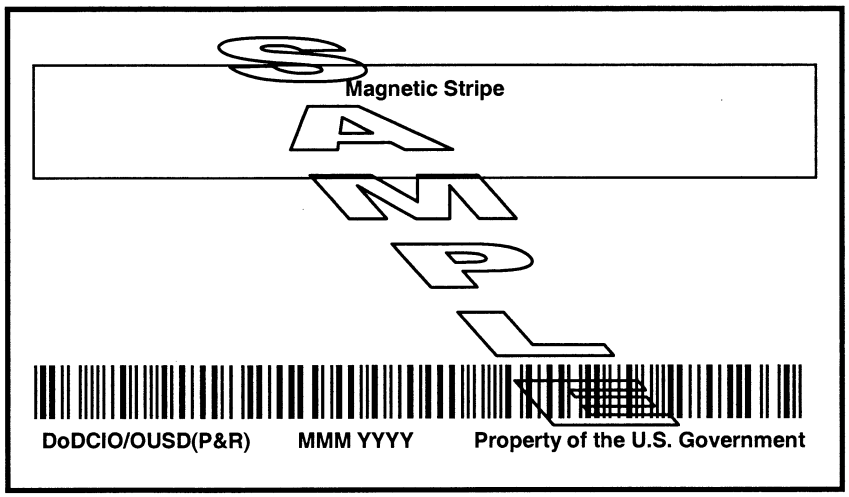
NOTES:

1. These Presidential Appointees are authorized medical and emergency dental care in military medical and/or dental treatment facilities within the Contiguous United States. Within the National Capital Region (NCR), charges for outpatient care are waived. Charges for inpatient and/or outpatient care provided outside the NCR will be at the interagency rates.

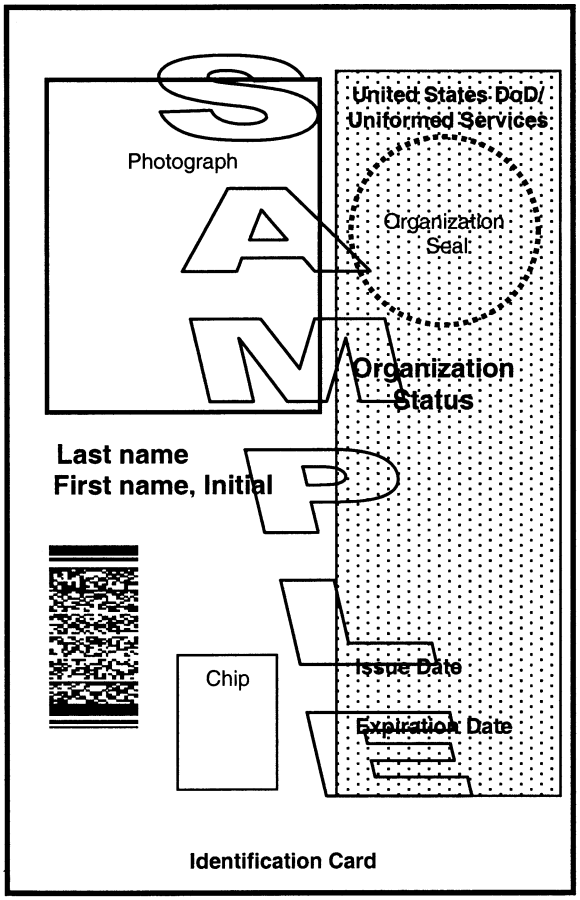
2. Exchange employees are entitled to all privileges of the exchange system, except for purchase of articles of uniform and state tax-free items.

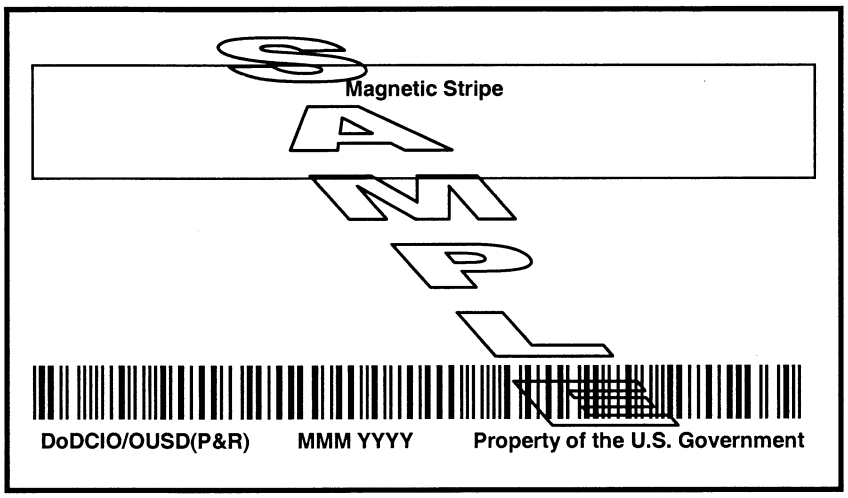
United States DoD/Uniformed Services Identification Card





United States DoD/Uniformed Services
Identification Card
With Color Band for Designated Contractor Employees
And Foreign Nationals





United States DoD/Uniformed Services Identification Card

The United States DoD/Uniformed Services Identification Card is the premiere of a DoD Identification Card for all civilian employees and contractor employees not eligible for the Identification and Privilege CAC. This card shall be the primary identification, and physical and logical access card for civilian employees in the following categories:

Civilian employees (see Definitions) to include:
- Individuals appointed to appropriated fund and nonappropriated fund positions
- Permanent or time-limited employees on full-time, part-time, or intermittent work schedules
- Senior Executive Service, competitive service, and Excepted Service employees

Contractor employees (see Definitions)

Civilian employees who operate RAPIDS workstations at Federal Agencies, other than DoD (i.e., NOAA, PHS, CG)

EXCEPTION: Since the Defense Eligibility Enrollment Reporting System (DEERS) is the platform from which the CAC is generated, and personnel information on employees of the Intelligence Community (e.g., National Security Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, and National Reconnaissance Office) is not maintained in DEERS, civilian employees of the Intelligence Community will not be issued a CAC.

In the Status area of the card, the card will show:

SES for Senior Executive Service employees
CIVILIAN for civilian employees, and
CONTRACTOR for contractor employees
FOREIGN NATIONAL for foreign national indirect hires

The expiration date on this card will be the earliest of three years or expected termination of the recipient's employment or association with the Department.

The CAC will also be used to facilitate standardized, uniform access to DoD facilities, installations, and computer systems.

When there are no communications either with the DEERS database or the DoD certificate authority, a temporary card can be issued with an abbreviated expiration date for a minimum of 10 and maximum of 280 days. The temporary card will not have a chip, nor will it have PKI certificates. The temporary card will appear the same as the United States DoD/Uniformed Services Identification Card with a white space where the chip is normally.

DEFINITIONS

Civilian Employee - DoD civilian employees, as defined in Title 5, United States Code, section 2105, are individuals appointed to positions by designated officials.

The appointments to appropriated fund positions either are 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.

The positions are categorized further as Senior Executive Service, competitive service, and excepted service positions. In addition, DoD employs individuals paid from non-appropriated funds, as well as foreign national citizens outside the United States, its territories, and its possessions, in DoD activities overseas. The terms and conditions of host nation citizen employment are governed by controlling treaties, agreements, and memorandums of understanding with the foreign nations.

Competitive Service Positions - Appointments to appropriated fund positions based on selection from competitive examination registers of eligibles or under a direct hire authority.
5 U.S.C. 2102

Contingency - means a military operation that (a) is designated by the Secretary of Defense as an operation in which members of the Armed Forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force; or (b) results in the call or order to, or retention on, active duty of members of the uniformed services under section 688, 12301(a), 12302, 12304, 12305, or 12406 of title 10, chapter 15, or any other provision of law during a war or during a national emergency declared by the President or Congress. *10 U.S.C. 101*

Contingency Contractor Employee - An employee of a firm, or individual under contract or subcontract to the DoD, designated as providing support or services vital to contingency, mobilization, or wartime missions. A contingency contractor employee must be located overseas or be subject to deployment overseas to perform functions in direct support of the essential contractor service.

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

Defense Agencies and Offices - All agencies and offices of the Department to Defense, including Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Contract Management Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency,

Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency/Central Security Service.

Essential Contractor Service - A service provided by a firm or an individual under contract to the DoD to support vital systems including ships owned, leased or operated in support of military missions or roles at sea and associated support activities including installation, garrison and base support services considered of utmost importance to the U.S. mobilization and wartime mission. That includes services provided to Foreign Military Sales customers under the Security Assistance Program. Those services are essential because of the following:

a. DoD Components may not have military or DoD civilian employees directly perform these services.

b. The effectiveness of Defense systems or operations may be seriously impaired, and interruption is unacceptable when those services are not available immediately. (Source: DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crises.")

Excepted Service Positions - All appropriated fund positions in the Department that specifically are excepted from the competitive service by or pursuant to statute, by the President, or by Office of Personnel Management, and which are not in the Senior Executive Service. Individuals also may be appointed to the competitive service by conversion from another appointment, such as a Veterans Rehabilitation Act appointment. Excepted service appointments include student career program appointments and student temporary employment program appointments.

5 U.S.C. 2103

Experts and Consultants

Expert Positions - Positions that require providing advice, views, opinions, alternatives, or recommendations on a temporary and/or intermittent basis on issues, problems, or questions presented by a federal official.

Consultant Positions - Positions that require the services of specialists with skills superior to those of others in the same profession, occupation, or activity to perform work on a temporary and/or intermittent basis assigned by a federal official. *5 CFR 304.102*

Foreign National Positions - Direct Hire - Non-United States citizens hired under an agreement with the host nation and paid and administered directly by the U.S. forces.

10 U.S.C. 1581

Foreign National Positions - Indirect Hire - Employees hired and administered by an entity other than the U.S. forces for the benefit of the U.S. forces. *10 U.S.C. 1581*

Foreign Military Personnel:

1. Sponsored North Atlantic Treaty Organization (NATO) and Partnership For Peace Personnel (PFP) 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 DoD or a Military Service.

2. Sponsored Non-NATO Personnel in the United States. Active duty officer and enlisted personnel of non-NATO countries serving in the United States under the sponsorship or invitation of the DoD or a Military Service.

3. 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 DoD or a Military Service, or when it is determined by the major overseas commander that the granting of such privileges is in the best interests of the United States and such personnel are connected with, or their activities are related to the performance of functions of the U.S. military establishment.

4. NOTE: 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 DoD or a Military Service ARE NOT ELIGIBLE FOR A CAC, and will continue to receive a DD Form 2765.

Full-time Work Schedule - Full-time employment with a basic 40-hour workweek.
5 CFR 610.111

Intermittent Work Schedule - Employment without a regularly scheduled tour of duty.
5 CFR 340.401

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. *5 CFR 315.608*

Nonappropriated Fund Positions - Nonappropriated Fund (NAF) employees are federal employees within the Department who are paid from nonappropriated funds. Title 5 United States Code, section 2105(c) explains the status of NAF employees as Federal employees.
DoD 1400.25-M Civilian Personnel Manual Subchapter 1401

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. *5 CFR 340.101*

Permanent Appointment - Career or career conditional appointment in the competitive or Senior Executive Service and an appointment in the excepted service that carry no restrictions or conditions. *5 CFR 340.202*

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

5 CFR 340.401

Senior Executive Service Positions - Appropriated fund positions in an agency classified above GS-15 pursuant to section 5108 or in level IV or V of the Executive Schedule, 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 which an employee performs the functions listed in 5 U.S.C. 3132. *5 U.S.C. 3132*

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

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

5 CFR 316.301

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. *5 CFR 316.301*

Volunteer Service - Services performed by a student, with the permission of the institution at which the student is enrolled, as part of an agency program established for the purpose of providing education experience for the student. Such service is to be uncompensated.

5 CFR 308.101