DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

November 26, 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
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

SUBJECT: Directive-Type Memorandum (DTM) 08-006 – "DoD Implementation of Homeland Security Presidential Directive - 12 (HSPD-12)"

References: (a) Section 3542(b)(2) of title 44, United States Code
(b) Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (FIPS 201-1), March 2006
(c) DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19, 2004

Purpose. This DTM establishes DoD policy for implementation of HSPD-12. This DTM is effective immediately; it shall be converted to a new DoD Instruction within 180 days.

Applicability. This DTM applies to 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 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.

Policy. HSPD-12 mandates a Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees under the terms of applicable contracts. HSPD-12 further directs Federal Departments and Agencies to migrate to a single identification standard for Federal employees and contractor employees under the terms of applicable contracts, for physical access to all Federally controlled facilities and logical access to Federally controlled information systems. "National security systems," as defined by section 3542 (b)(2) of title 44, United States Code (Reference (a)), and "Special-Risk Security Provisions," as defined by Federal Information Processing Standard 201-1 (FIPS 201-1) (Reference (b)), are exempted from this policy.

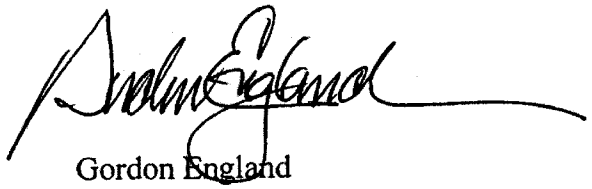
The Common Access Card (CAC) is the DoD Federal credential, and as such, effective immediately and consistent with applicable law, the CAC will be accepted by all DoD Components as the official DoD/Federal identification credential that can be used for logical and physical access once access privileges are granted. These credentials do not automatically grant access to either Federally controlled facilities or information systems. The granting of access privileges is determined by the facility or system owner as prescribed by DoD policy, issued by either the Under Secretary of Defense for Intelligence (USD(I)) for facility access, the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) for system access, or the Under Secretary of Defense for Policy (USD(P)) in support of the Department's Antiterrorism Program. Phased upgrades to Real-time Personnel Identification Systems (RAPIDS) sites have been initiated so that certain changes to the CAC and its issuance processes, which are required to comply fully with HSPD-12, can be achieved in accordance with the governing standard (Reference (b)). The Department of Defense's strategy is to issue compliant credentials as RAPIDS sites are upgraded and existing credentials expire over the next 4 years.

Responsibilities. To ensure successful DoD migration to the HSPD-12 credential, the identified OSD Principal Staff Assistants will issue policy per the responsibilities outlined in the attachment and consistent with Department of Defense HSPD-12 Implementation Plan. These HSPD-12 responsibilities are assigned, consistent with existing policies on the broad responsibilities of the OSD Principal Staff Assistants. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will develop and coordinate the DoD Instruction to incorporate this DTM into an existing DoD issuance or convert to a new issuance.

Procedures. Uniformed Service members, civilian employees, Presidential Appointees, or CAC-eligible contractor employees under the terms of applicable contracts will need to have an initiated National Agency Check with Inquiries (NACI); National Agency Check, Law Checks, and Credit, or an initiated national security investigation; and a favorable completion of a Federal Bureau of Investigation (FBI) fingerprint check for credential issuance. The USD(P&R), DoD lead for HSPD-12, will work with the Office of Personnel Management to integrate the NACI status and fingerprint check information into the CAC issuance process.

The points of contacts for this effort are Ms. Heidi Boyd (Heidi.Boyd@osd.pentagon.mil, 703-696-0404) for USD(P&R); Ms. Donna Rivera (Donna.Rivera@osd.mil, 703-604-1172) and Ms. Andrea Upperman (Andrea.Upperman@osd.mil, 703-604-1112) for USD(I); and Col Richard D. McComb (Richard.mccomb@osd.mil, 703-697-0742) or Mr. Anthony Fortune (Anthony.Fortune@osd.mil, 703-602-5730 extension 142) for USD(P).

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.



Gordon England
Deputy Secretary of Defense

Attachment:
As stated

ATTACHMENT

RESPONSIBILITIES

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

a. Consistent with Privacy Act requirements, electronically capture and store source documents in the identity proofing process at the accession points for eligible credential holders.

b. Implement modifications to the CAC applets and interfaces.

c. Consistent with Privacy Act requirements, implement modifications to the CAC topology.

d. Add contactless capability to the CAC platform.

e. Establish interface with OPM for access to the Clearance Verification System to determine suitability for credentialing.

f. Advise DoD Components processing new hires or new military accessions to allow 1 week prior to hiring or accessing for completion of fingerprint check to avoid delay in issuing an interim CAC.

g. In coordination with USD(I), ASD(NII)/DoD CIO, and Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), establish policy and oversight for FIPS 201-1-compliant CAC issuance.

h. In coordination with USD(I) and DoD General Counsel (DoD GC), identify an adjudication process for individuals when disqualifying information is developed from FBI fingerprinting, NACI, or other applicable background checks.

i. In coordination with USD(I) and DoD GC, establish an appeals process for denials or revocations of the Personal Identity Verification card.

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

a. Issue regulatory coverage for contracts.

b. Communicate HSPD-12 requirements to the DoD Acquisition community.

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

a. Establish guidance for the use of the CAC for physical access purposes for both DoD and Interagency use.

b. Establish guidance in the security community for verifying the authenticity and validity of Federal credentials for physical access.

c. Establish guidance for visual and electronic authentication of credentials within the physical security community.

d. Establish guidance and process for cross-acceptance of FIPS 201-1-compliant credential of other Federal agencies when visiting DoD facilities or controlled spaces.

e. In coordination with the OSD PSA for Biometrics (Director, Defense Research & Engineering), DoD GC, and the DoD Executive Agent for Biometrics, determine the policy for incorporation of biometrics into intelligence, personnel security, and physical security requirements and capabilities.

f. Provide policy on physical security standards (access control equipment) to the acquisition community for FIPS 201-1 credentialing and visitor badging.

g. Establish guidance for Special-Risk Security Provision authorizations as described in Reference (b).

h. In coordination with USD(AT&L) and DoD GC, establish policy for contractor employees under the terms of applicable contracts that supports background vetting in compliance with HSPD-12.

i. In coordination with USD(P&R) and DoD GC, establish policy for military and civilians that supports background vetting in compliance with HSPD-12.

j. In coordination with USD(P&R), DoD GC, and USD(AT&L), establish a centralized approach for the vetting submission and adjudication for interim credentialing across the Department of Defense.

k. In coordination with USD(AT&L), establish hardware requirements for HSPD-12 compliance.

l. Coordinate with the USD(P) activities affecting the DoD Antiterrorism Program.

4. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall:

a. Modify certificate fields or certificate profiles, if required, to comply with Reference (b) requirements.

b. Modify certificate revocation lists, if required, to comply with Reference (b) requirements.

c. Establish a formal relationship between the Federal Bridge Certification Authority and the Department of Defense, and exchange the appropriate cross-certificates required to comply with Reference (b).

d. Map the current DoD Public Key Infrastructure (PKI) certificates to those required within Reference (b).

e. Facilitate the addition of any new Reference (b)-required certificates.

f. Modify PKI applet interfaces and structures.

5. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE & AMERICAS' SECURITY AFFAIRS) (ASD(HD&ASA)). The ASD(HD&ASA), under the authority, direction, and control of USD(P), shall facilitate force protection activities with the law enforcement community.

6. DoD IDENTITY PROTECTION AND MANAGEMENT SENIOR COORDINATING GROUP. The DoD Identity Protection and Management Senior Coordinating Group, under joint oversight of USD(P&R) and ASD(NII)/DoD CIO, shall monitor the activities outlined within this attachment in accordance with DoD Directive 1000.25 (Reference (c)).