DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT GORDON
307 CHAMBERLAIN AVENUE
FORT GORDON, GEORGIA 30905-5730

REPLY TO
ATTENTION OF:

IMSE-GOR-HR

JUN 28 2010

MEMORANDUM FOR All Fort Gordon Personnel

SUBJECT: Garrison Commander's Policy Memorandum No. 57 — Common Access Card (CAC) Procedural Guidance for the Contractor Verification System (CVS)

1. References.

a. Under Secretary of Defense Memorandum, "Directive-Type Memorandum (DTM) 08-003, 'Next Generation Common Access Card (CAC) Implementation Guidance,'" 1 December 2008.

b. Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Implementation of Homeland Security Presidential Directive-12 (HSPD-12)," 26 November 2008.

c. Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," 27 August 2004.

d. Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," 1 March 2006.

2. Purpose. To provide procedural guidance for issuing CAC to DoD Contractor personnel.

3. Applicability. This policy memorandum applies to all organizations and activities operating on Fort Gordon.

4. Background. Reference (c) mandated an establishment of "a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees)." Reference (b) 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. The government wide standard is the Federal Information Processing Standards (FIPS) Publication (PUB) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, originally published 25 February 2005, provided the following milestone: Federal departments and agencies shall meet the requirements of PIV-I no later than 27 October 2005, in accordance with the timetable specified in HSPD 12. The PIV-I included the background vetting requirement. The CAC is DoD's PIV compliant identity credential.

5. Responsibilities. See Enclosure.

6. Procedures. The new procedural guidelines are effective immediately. 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; and (d) verification of a claimed identity.

a. CAC Eligibility. A CAC will be issued to only those DoD Contractors with a requirement to access Fort Gordon facilities and networks. CAC eligibility for DoD Contractors is based solely 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:

(1) 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).

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

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

b. Background Vetting.

(1) DoD Contractors will not be issued a CAC without the required background vetting. 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.

(2) 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. Government sponsors are responsible for ensuring that the vetting requirements have been met before approving CAC issuance for all Contractors. Government sponsors should refer to their employer organizations and local personnel security offices, as well as OPM Federal Investigations Notice 06-04, 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.

c. Expiration Date. CACs will be issued for a period not to exceed three (3) years from the date of issuance or contract expiration date, whichever is sooner. *Non-deploying Contractors*: Enter the date of the current contract period of performance. 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. *Deploying Contractors*: Enter the deployment end date.

d. Reverification. CVS reverification actions did not have sufficient evidence to support the Contractors' continued need for CACs. Army CVS Trusted Agents shall require electronic confirmation from the Contractor company that the individual Contractor has a continued need for the CAC. This confirmation may be an email or may be a recurring report from the Contractor company updating the list of Contractors providing support. Electron documentation should be retained until superseded by a subsequent report, or the CAC expires or is revoked.

7. Proponent for this policy is the Directorate of Human Resources at (706) 791-2914, (706) 791-3914, or (706) 791-6776.

Encl

GLENN A. KENNEDY, II
COL, SC
Commanding

Enclosure

Responsibilities

1. **Fort Gordon Commanders, Directors, and Principal Staff Officers.** All Fort Gordon components shall:

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

b. Ensure contract support and other affiliate CAC applicants have met background investigation requirements outlined within paragraph six (6) of policy memorandum prior to approving CAC sponsorship and authorization.

c. 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 and DoD 5200.1-R. These cards shall be returned to Darling Hall, Building 33720, Room 161 or any RAPIDS issuance location for proper disposal.

d. 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.

2. **CVS Trusted Agent Security Manager (TASM).** All TASMs have specific security requirements. You must be vetted in accordance with Department of Defense (DoD) Directive 5200.2-R, "DoD Personnel Security Program," because you are seeking access to information protected under the Privacy Act or sensitive Personally Identifiable Information (PII). It is expected that you are trustworthy, maintain a good working knowledge of site operations, and meet the security requirements for your site. TASM's will:

a. Ensure efficiency and security at your site when granting Defense Manpower Data Center (DMDC) application access to users.

b. Protect Privacy Act and Personally Identifiable Information (PII) using DMDC Security Online.

c. Maintain your annual site security managers (SSM) training certification for DMDC Security Online.

d. Initiate, maintain and document personnel security investigations appropriate to the individual's responsibilities and access to DMDC information, using an authoritative source such as the Defense Security Service (DSS) or the Office of Personnel Management (OPM).

e. Immediately report to the appropriate government representative if any person filling a sensitive position receives an unfavorable adjudication or if information that would result in an unfavorable adjudication becomes known.

f. Immediately deny DoD Assurance Information Systems (AIS)/network and DMDC information access to any personnel receiving an unfavorable adjudication at any time or if directed to do so by the appropriate government representative.

g. Ensure all personnel receive information assurance security training before being granted access to any DoD AIS/network or DMDC information.

h. Ensure that each person has completed and submitted Standard Form 85-P, "Questionnaire for Public Trust Positions," fingerprint forms and other such documentation as the OPM requires for its investigation.

i. Interim (temporary) access may be provided while the investigation is ongoing, per guidance in DoD directive 5200.2-R. Only U.S. citizens—including temporary, intermittent, and seasonal personnel—may be vetted at IT-I or IT-II levels on an interim basis before a final adjudication, per DoD directive 5200.2-R.

3. **CVS Trusted Agent (TA)**. The TAs primary role is threefold: begin the process of establishing a Contractor's identity in DEERS; verify the Contractor's need for logical or physical access to either a DoD network or facility; and establish sponsorship of the Contractor with the Service or Agency. TAs have several general responsibilities including:

a. Meeting TA Position Requirements

b. Ensuring positive identification of all Applicants requesting a government credential

c. Ensuring Applicants have gone through the proper vetting process

d. Notifying the TASM of site capability outages

e. Notifying the TASM, SPOC, or DSC of any suspected or known CVS system compromise

f. Notifying the TASM (or DSC if local TASM is unavailable) of any malfunctions or anomalies with CVS

g. Performing the TA Specific Responsibilities

(1) Provide Applicant access to CVS

(2) Review completed Contractor application forms

(3) Verify an Applicant's need for a government credential

(4) Approve or reject the Contractor's application

(5) Reverify assigned Applicants by confirming the Applicant's continued affiliation with the DoD

(6) Revoke a Applicant's need for a government credential

(7) Complete the CVS Certification Training