



**DEPARTMENT OF THE ARMY**  
US ARMY INSTALLATION MANAGEMENT COMMAND  
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT BELVOIR  
9820 FLAGLER ROAD, SUITE 213  
FORT BELVOIR, VIRGINIA 22060-5928

REPLY TO  
ATTENTION OF

IMBV-HR

12 August 2016

MEMORANDUM FOR US Army Fort Belvoir Garrison Personnel and Mission Partners

SUBJECT: Fort Belvoir Policy Memorandum #55, Common Access Card (CAC) Credentialing and Installation Access for Uncleared Contractors

1. REFERENCES.

- a. Army Directive 2011-08 (Army Implementation of Homeland Security Presidential Directive-12), 26 May 2011.
- b. Army Directive 2014-05 (Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors), 7 March 2014.
- c. Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System (TASS) Trusted Agent (TA/Trusted Agent Security Manager (TASM) User Guide, October 2014.
- d. Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System Overview Guide, June 2014.
- e. DoDM 1000.13, Volume 1 and Volume 2, (DoD Identification (ID) Cards: ID Card Life-Cycle), 23 January 2014.

2. PURPOSE. Prescribe procedures and responsibilities for the Common Access Card (CAC) credentialing and installation access for uncleared contractors.

3. APPLICABILITY. This policy pertains to all Fort Belvoir Garrison personnel and mission partners.

4. POLICY. All contractors will comply with the requirements for Common Access Card (CAC) credentialing and installation access onto Fort Belvoir facilities and/or networks.

5. PROCEDURES.

a. CAC Eligibility.

(1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely.

(2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures.

(3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of six months or more.

**“LEADERS IN EXCELLENCE”**

IMBV-HR

SUBJECT: Fort Belvoir Policy Memorandum #55, Common Access Card (CAC) Credentialing and Installation Access for Uncleared Contractors

b. Roles and responsibilities.

(1) All TAs, TASMs and Contracting Officer Representatives (CORs) must meet all requirements for appointment to these roles, to include required training and certifications.

(2) The COR is responsible for notifying the TA within the organization of the new contractor needing a CAC. COR will retrieve CAC from contractor upon termination or expiration of contract.

(3) The TA is responsible for submitting the new contractor personnel information into the TASS for vetting to obtain a CAC. TA is responsible for submitting the contract number and expiration date of the contract. Once TA has received in writing from Security Officer vetting process is complete and favorable, TA will complete application in TASS authorizing issuance of CAC. Once the contract is either terminated or contracting requirement is completed due to expiration date, the COR will retrieve CAC and return to TA. The TA will turn CAC in to the TASM.

(4) The Security Officer is responsible for vetting new contractors. Once background investigation is complete and finding is favorable or not favorable; Security Officer will provide in writing the results to the TA.

(5) The TASM is responsible for granting access to new TAs and providing training and materials. Ensure TAs have met required certification and conduct monthly audits, to ensure TAs are performing duties IAW Army Directive 2011-08, Army Implementation of Homeland Security Presidential Directive-12. TASM is responsible for returning all retrieved CACs from TAs to local ID Card facility.

c. CAC credentialing.

(1) Initial CAC issuance can be made after the following has been completed:

(a) National Agency Check with Inquiries (NACI) has been accepted by Office of Personnel Management (OPM) and a favorable review of the SF 85 Questionnaire for Non-Sensitive Positions has been made by Directorate of Plans, Training, Mobilization and Security (DPTMS) Security Division.

(b) Favorable Federal Bureau of Investigation (FBI) Fingerprint results have been received/reviewed by DPTMS Security Division.

(c) Proof of Identity (driver's license/identification card/passport/citizenship documentation with photo) has been presented to the DPTMS Security Division.

IMBV-HR

SUBJECT: Fort Belvoir Policy Memorandum #55, Common Access Card (CAC) Credentialing and Installation Access for Uncleared Contractors

(d) The TA will receive notification in writing from the security officer that the fingerprint and NACI background investigation is complete.

(2) Office of Personnel Management and Department of the Army supports reciprocity on previously conducted investigations. Provided investigation results are available, individuals who have a completed clean or favorably adjudicated NACI or higher investigation without a twenty four month break in service will not require reinvestigation upon employment.

d. To ensure quality assurance, the installation's TASM will conduct monthly inspections with TAs to verify the vetting process and report findings to the Garrison Commander.

e. Commanders and ID Card issuing facilities/agencies will not authorize issuance of CACs to individuals ineligible for credentialing, nor approve exceptions, in lieu of complying with access control policy and NCIC-III vetting requirements.

f. A current listing of Trusted Agents (TAs), Trusted Agent Security Managers (TASMs) and Contracting Officer Representatives (CORs), along with copies of appointment memorandums, must be provided to the Installation TASM, Ms. Glenda L. Payne, [glenda.l.payne.civ@mail.mil](mailto:glenda.l.payne.civ@mail.mil).

g. The Directorate of Emergency Services is responsible for installation access for all non-CAC contractors. Installation access can be coordinated through the SSG John D. Linde Visitor Center located at Tulley Gate, 703-806-4892.

6. PROPONENT. The proponent for this policy is the Directorate of Human Resources at 703-805-1053.



ANGIE K. HOLBROOK  
Colonel, AG  
Commanding