DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT DRUM
10000 10TH MOUNTAIN DIVISION DRIVE
FORT DRUM, NEW YORK 13602-5046

AMIM-DRG-ZA 11 March 2022

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Garrison Policy Memorandum 21-20, Common Access Card Credentialing for Eligible Department of Defense (DoD) and Other Federal Contractors

1. References:

a. DoD Instruction 5200.46, DoD Investigative and Adjudication Guidance for Issuing the Common Access Card (CAC), with Change 2, 2 November 2020.

b. DoD Manual 1000.13, Volume 1, DoD Identification Card (ID): ID Card Life -Cycle, with Change 1, 28 July 2020.

c. Army Regulation 600-78, Army Suitability Program, 25 October 2018.

d. Army Regulation 190-13, The Army Physical Security Program, 27 June 2019.

e. Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System (TASS) Overview Guide Version 7.2, December 2020.

2. Purpose: To establish Fort Drum policy and responsibilities concerning the CAC Credentialing Program for eligible DoD and Federal contractors**.**

3. Applicability: This memorandum applies to all DoD and Federal contractors on Fort Drum.

4. General:

a. Sponsorship and Eligibility: DoD and Federal contractors requiring access to Fort Drum require a government sponsor. The sponsor is a person affiliated with the DoD who takes responsibility for verifying and authorizing the applicant's requirement for a government issued CAC. Applicants for a CAC must be sponsored by a DoD government official or employee.

b. Sponsoring organizations will establish procedures to ensure that the issuance and retrieval of a CAC is part of the normal personnel in-processing and out-processing requirements within the organization, and that internal controls are in place to monitor the application and re-verification process. The government employees with primary responsibility to ensure eligibility, completion of the application, and CAC turn-in are the

applicant's Contracting Officer's Representative (COR) and Trusted Agent (TA). The COR and TA may be the same individual.

c. A CAC eligible applicant is defined as any U.S. or Foreign National person who is authorized and requires access to multiple (two or more) DoD-controlled installations or facilities on behalf of the Department of the Army (DA) on a recurring basis for a period of six months or more; or requiring both access to a DoD controlled installation or facility and onsite or remote access to DoD or DA controlled information networks.

5. Responsibilities:

a. The Commander/Director will:

(1) Establish an Industrial Security Program for contractors in their command, activities, and areas of responsibility.

(2) Ensure local Supporting Security Managers (SSMs), Trusted Agent Security Managers (TASMs), TAs, and CORs abide by this policy and meet training requirements.

(3) Ensure prompt reporting of credible derogatory information on all personnel, to include embedded/integrated contractors.

(4) Ensure in-processing and out-processing procedures support the guidance in this policy.

b. The COR will:

(1) Be a federal employee with at least a favorable National Agency Check with Inquiries (NACI) for unclassified contracts; be a federal employee with a minimum security clearance level commensurate with the classification level of the classified contract.

(2) Notify the TA within the organization of a new contractor employee needing a CAC and assist with providing necessary documentation for security verification.

(3) Retrieve the CAC from the contractor employee upon termination of the contract or termination of employment.

(4) Work with supporting contracting commands to ensure CAC security clauses and retrieval responsibilities are incorporated in the contract performance work statement.

(5) Complete section II of the applicant's Army Human Resources Command (AHRC) TASS Form 1 (see enclosure) and submit it to the local SSM.

(6) Refer the contractor to the appropriate local SSM for completion of a Contractor Verification Memo (CVM) if it does not have a TASS Form 1 (e.g. non-Army agencies and regional contractors).

c. The Local Supporting Security Manager will:

(1) Be a federal employee with at least a secret clearance and active CAC.

(2) Review Defense Information System for Security (DISS) records for all contractor employees receiving a CAC.

(3) Complete section III of the AHRC TASS Form 1 and submit it to TA.

(4) Provide a CVM to the Fort Drum Directorate of Human Resources (DHR) DEERS/ID Center prior to it issuing a contractor employee a CAC card.

(5) Provide in-processing and out-processing in the appropriate category in DISS for contractor employees.

(6) Facilitate appointments for Federal Bureau of Investigation (FBI) fingerprint Special Agreement Checks, with the appropriate Command Security Manager/ Office, for contractor employees.

(7) Report derogatory information and revoke CAC credentials when required.

d. The TA will:

(1) Be a federal employee with at least a favorable NACI and a current CAC.

(2) Determine initial CAC eligibility in conjunction with the sponsoring agency and then reconfirm eligibility every 180 days to ensure only authorized individuals are issued a CAC.

(3) Ensure an applicant is vetted through the SSM with a favorable FBI fingerprint Special Agreement Check (SAC) and NACI on file. This verification will be provided to the TA from the SSM in writing on TASS Form 1.

(4) Process and approve applications for a CAC following the procedures in the most current TASS, TA, and TASM user guides.

(5) Take immediate action to revoke a CAC when eligibility no longer exists.

(6) Return expired and/or turned in CACs to the DHR DEERS/ID Center.

(7) Maintain less than one hundred active CACs.

(8) Report any adverse information, suspicious contacts, or other reportable incidents by submitting information and any documents in writing to the COR and the SSM.

(9) Follow up on interim credentialing decisions every thirty days.

(10) Brief CAC applicants on the following:

(a) Their responsibility to account for and protect the CAC.

(b) Their responsibility to return the CAC to the sponsoring organization upon expiration of the CAC, contract expiration, termination of employment, or when the CAC is no longer needed for DoD network access or access to a DoD facility.

(c) The CAC is only authorized for use for the specific contract for which it was issued, unless written authorization for alternative use is received from the COR; for instance, the contractor cannot use the CAC to visit another military installation unless authorized in writing by the COR.

e. The DHR DEERS/ID Center will:

(1) Check TASS for applicant approval by the TA.

(2) Verify that an approved Contractor Verification Memo (CVM) was received from the local SSM. The CVM can be hand-carried by the applicant, or emailed from the local SSM directly to the DEERS/ID Center.

(3) The DEERS/ID Center will not provide initial CAC services to <u>any</u> contractor personnel until a local SSM has vetted them and provided a CVM confirming their eligibility status. The CVM is in addition to the need for the contractors TA to generate a TASS Form 1 and input them in TASS.

(4) Issue CACs.

f. The TASM will:

(1) Be a federal employee with at least a favorable NACI and a current CAC.

(2) Grant access to new TAs and provide training and materials.

(3) Ensure TAs meet certification requirements.

(4) Conduct monthly audits of TAs to ensure compliance with this policy.

(5) Perform duties as TA if required.

6. CAC Credentialing:

a. An interim CAC credential is authorized and may be issued when a favorable FBI fingerprint SAC and Tier 1 Homeland Presidential Directive (HSPD) -12 NACI has been received by the Personnel Security Investigation Center of Excellence (PSI-CoE), and it has initially been adjudicated as favorable.

b. A Final CAC credential is authorized when DISS records show that a Tier 1 Homeland Presidential Directive (HSPD) -12 NACI has been completed by the Office of Personnel Management (OPM) and adjudicated favorably by the Department of Defense Central Adjudication Facility (DoDCAF).

c. OPM and DA support reciprocity on previously conducted federal security investigations/inquiries. Provided the previous investigation/inquiry results are available, the subject of the investigation/inquiry received a favorably adjudicated NACI or higher investigation, and there is less than a twenty four month break in the subject's service under a federal contract, a new investigation/inquiry will not be required upon re-employment under a federal contract. Contractor employees that require a security clearance must have a National Agency Check with Law and Credit (NACLC) or higher investigation.

d. When the expiration date of a CAC approaches and the contractor employee has a continuing requirement to possess a CAC (i.e. continue contract performance), the employee must apply for a new card. The COR must verify the requirement for a new card according to policies and procedures current at the time of the application.

e. When a determination is made to deny or revoke a CAC, the applicant or cardholder will be afforded due process in accordance with procedures outlined in Army Regulation 190-13.

7. CAC retrieval:

a. Sponsors will retrieve CACs issued to contractor employees upon completion of the contract, termination of employment, denial or revocation as a result of a final credentialing determination, or when an employee no longer meets the eligibility requirements in paragraph 3b above.

b. Sponsors will give retrieved CACs to the TASM or TA, who will return the CACs to the DHR DEERS/ID Center using a DA Form 200, transmittal record. The DHR DEERS/ID Center may grant TASMs and TAs front of the line privileges when returning CACs.

c. If the CAC cannot be retrieved, the sponsor or contractor site lead, or equivalent, will immediately provide a memorandum to the DHR DEERS/ID Center and to the TA explaining why the CAC could not be retrieved. Upon receipt of this memorandum, the TA will immediately revoke the CAC in TASS and send the memorandum to the Network Enterprise Center (NEC) to void its certificates, and to the Directorate of Emergency Services (DES). DES will enter this information into their installation access database.

10. If a CAC is lost, stolen, or destroyed, contractor personnel will submit a Military Personnel Division (MPD) Form 506-E, Statement of Lost, Stolen or Damaged ID Card. The TA will re-verify vetting with the local SSM and process a new CAC application in TASS once a new TASS Form 1 is received.

11. The TASS proponent for this policy is the Director, Human Resources, at (315) 772-3193.

ZACCHINO.JAMES.JOSEPH.JR.1036377336
Digitally signed by ZACCHINO.JAMES.JOSEPH.JR.1036377336
Date: 2022.03.14 09:17:52 -04'00'

Encl
as

JAMES J. ZACCHINO, JR.
Colonel, LG
Garrison Commander

DISTRIBUTION: A