DEFENSE COMMISSARY AGENCY
HEADQUARTERS
1300 E AVENUE
FORT LEE, VIRGINIA 23801-1800

IN REPLY
REFER TO

COP

February 11, 2015

NOTICE TO THE TRADE-DECA NOTICE 15-30

SUBJECT: Fort Lee Criminal Background Checks for Non-DoD ID Cardholders

REFERENCE: (a) Fort Lee Operations Order 15-010, Security Verification of non-CAC-Eligible Contractors
(b) Fort Lee Traveller, "New access requirements to enhance post security," January 29, 2015

The purpose of this "Notice to the Trade" is to alert industry partners, vendors and contractors to new gate security measures at Fort Lee scheduled to go into effect April 15, 2015. The measures, directed by the Department of the Army, enact more stringent regulatory requirements, specifying that individuals who do not possess Department of Defense identification must submit to a criminal background check before they are permitted to enter the installation.

Within the next few weeks DeCA will be coordinating with the Fort Lee installation a list of contractors, civilian employees and vendors who are not eligible to receive a Common Access Card but work within or who regularly visit the Headquarters or commissary. As further details are released, we will notify industry of which DoD credentials are authorized for gaining entry to the installation, and the procedures Fort Lee will require to perform background checks on individuals who do not possess such credentials. It is our understanding that once the installation receives an individual's information, Fort Lee will perform the necessary background check, and that vetted individuals will receive an authorization letter that may be used to enter the installation.

If visitors do not have the proper access credentials once the new security measures begin, they will have to go to the Visitor Control Centers at the Lee and Sisisky gates. Beginning April 15, the background checks will be conducted at the Lee Gate, 6 a.m. – 8 p.m., Monday – Friday, and at the Sisisky Gate, 8 p.m. – 6 a.m., Monday – Friday.

We understand there may be many questions, and as we receive additional details we will share them with you. My points of contact are Timothy C. Ford at (804) 734-8000, extension 48552 or timothy.ford@deca.mil, and Beverly J. Clark at extension 48709 or beverly.clark@deca.mil.

Christopher T. Burns
Chief Performance Officer

USAG, Fort Lee
04 FEB 2015
S: 13 Feb 2015

OPERATIONS ORDER 15-010: Security Verification of non-CAC-Eligible Contractors (U)

Refs: (a) (U) Army Directive, Subject: 2014-05 (Policy and Implementation for Common Access Card Credentialing and Installations Access for Uncleared Contractors, dtd 7 Mar 14
(b) (U) Army Regulation, 190-13, The Army Physical Security Program Chapter 8, dtd 25 Feb 11
(c) (U) IMCOM OPORD 15-031 Implement Access Control Procedures at IMCOM Installations, dtd 211313Z Nov 14
(d) (U) HQDA EXORD 033-15 Installation Access (Directed Actions), dtd 7 Nov 14
(e) (U) Validation of the Office of the Provost Marshal General and Installation Management Command Common Levels of Support 600, Physical Security Manpower Mode, dtd 21 Nov 14
(f) (U) FRAGMENTARY ORDER 01 to OPERATIONS ORDER 15-031: Implement Access Control Procedures at IMCOM Installations, DTG 151313Z DEC14

(U) Time Zone Used Throughout the Order: Local.

1. (U) **SITUATION**.

1.A. (U) The Secretary of the Army directed the Office of the Provost Marshal General (OPMG), Army G-2, Army Audit Agency and the Inspector General to assess the Army's overall protection posture concerning Common Access Card (CAC) Credentialing and Access Control. Prior to their final reports, the Secretary of the Army published Army Directive (AD) 2014-05, ref (a) directing Army installations to review and implement policies concerning the issuance/control of CAC credentials and minimum standards for accessing Army Installations.

1.B. (U) All agencies reported that there were inconsistent standards for Access Control Points (ACPs), Visitor Control and CAC procedures across the Army. Their reports recommended several corrective actions directed towards IMCOM Garrisons.

2. (U) **MISSION**. The requirement to conduct vetting of non-CAC-eligible personnel will be executed in four (4) phases. Not later than (NLT) Close of Business (COB) 13 Feb 15, all Garrison Directorates and tenant organizations with non-CAC-eligible

personnel that could include contractors, volunteers, civilian employees and vendors will provide a Point of Contact (POC) from the Sponsoring Agency (SA) or Contracting Officer Representative (COR) and number of non-CAC- eligible personnel to the DES/PMO

A "non-CAC-eligible" person is defined as any U.S or Foreign National who is authorized and requires access to facilities on behalf of the Department of the Army on a recurring basis for a period of 6 months or more or requires both access to a facility and onsite service on the installation.

3. (U) **EXECUTION**.

3.A. (U) Commander's Intent. In coordination with the Senior Commander, my intent is to verify and ensure that all non-CAC-eligible personnel of organizations meet the criteria for admittance and work on Fort Lee and report to IMCOM HQ that all non-CAC eligible personnel of supported organizations have been checked and verified. The DES will inform organization POCs of verification results. The organization's POCs or COR will coordinate to have non-CAC-eligible personnel admittance revoked who do not meet the investigative criteria at a date to be determined.

3.B. (U) Concept of Operations. This execution of this requirement will be in four (4) phases.

PHASE I: Garrison Directorates and tenant organization will provide a POC from the SA or COR and number of non-CAC-eligible personnel that could include contractors, volunteers, and vendors (only numbers for each category is required at this time) NLT 13 Feb 15. POC to submit numbers is MAJ Joseph Tull, 734-7402, joseph.a.tull.mil@mail.mil.

PHASE II: Garrison Directorate and tenant organization POCs (SA or COR) will provide a by-name list of non-CAC-eligible personnel at a date to be determined.

PHASE III: The DES/PMO will complete vetting of all submitted non-CAC-eligible personnel and work with organizational POCs (SA or COR) if any vetted personnel require adjudication to determine final eligibility. Procedures will be sent to organizational POCs in a subsequent FRAGO to this ORDER.

PHASE IV: DES/PMO will coordinate with organizational POCs (SA or COR) for the date and time to issue access control credentials for non-CAC-eligible personnel.

3.C. (U) Coordinating Instructions.

3.C.1. (U) This order is effective upon publication.

4. (U) **SUSTAINMENT**. None.

5. (U) **COMMAND AND CONTROL**.

5.A. (U) <u>Command</u>. None

5.B. (U) <u>Control</u>. None.

5.C. (U) <u>Signal</u>. POCs is MAJ Joseph Tull, Provost Marshal, 734-7402, joseph.a.tull.mil@mail.mil.

ACKNOWLEDGE:

                        BROOKS
                        COL
                        Commanding

OFFICIAL:

BROWN
DPTMS
GS-14

DISTRIBUTION:
All Garrison Directorates
392d Army Band
217th MP Det
345th TRS
82d STB-FWD
AAFES
LESD
CASCOM
CID
Commissary
CPAC
LOGSA
DAU
DCMA
DECA
DENTAC
KAHC

DLA
DMPO
LRC
MEPS
MICC
NEC-LEE
SEC-LEE
USAFMSA
USAISEC
USATDS
USMC Det
USPS
VETCOM
VIB BSC
94th TD
Ft Lee Credit Union
Sun Trust Bank
Red Cross

New access requirements to enhance post security

T. Anthony Bell, Senior Writer - Special Projects | Posted: Thursday, January 29, 2015 12:00 am

FORT LEE, Va. (January 29, 2015) -- Fort Lee is slated to operate under new gate security measures beginning in April.

The measures, directed by the Department of the Army, fulfill more stringent regulatory requirements to vet non-Department of Defense identification cardholders prior to entering the installation. Current policies require only a state driver's license or a state identification card to gain entrance.

"The new policy requires us to perform a criminal background check for those who have not been appropriately vetted," said Tony DeWitt, director of the Emergency Services division here.

The measures will not hinder installation access by DOD ID cardholders and those who regularly visit the installation such as volunteers and some contract workers, DeWitt said.

New access requirements to enhance post security

Department of the Army Security Guard Mark Helber checks the identification of a motorist at the Lee Avenue Gate on Jan. 27. In mid-February, the Directorate of Emergency Services will begin implementing new DA requirements to perform background checks on non-DOD identification card holders.

Under the new security requirements, Fort Lee has plans to build a Visitor Control Center that will house several National Crime Information Center terminals to generate the criminal background checks, DeWitt said. Construction for the facility is scheduled to begin sometime in fiscal 2016.

Until the permanent facility is complete, the Lee Avenue and Sisisky Boulevard gates will handle VCC operations. The Lee gate is scheduled to begin VCC operations April 15. It will open from 6 a.m. - 8 p.m., Monday-Friday. The Sisisky gate VCC also is scheduled to come online in April. Its hours will be 8 p.m. - 6 a.m. on weekdays. Sisisky Gate itself serves as the installation's main gate and is always open to include weekends and holidays.

The VCC operation at the Lee gate will operate in a way that is similar to the current traffic configuration there, which was recently implemented due to unrelated construction projects at the Sisisky gate. It consists of three lanes of traffic – two that lead directly to the guard shacks – and one that loops in front of the Welcome Center facility. Non-DOD ID cardholders will use the third lane and that facility's parking area to check in and receive their background checks.

The traffic configuration at the Sisisky gate also will be modified. Details on those changes are still forthcoming, but the impact of VCC operations there is likely to be minimal compared to the Lee gate.

"We hope that our regular ID cardholders come through Sisisky gate during the duty day." DeWitt said. "It can better deal with the volume compared to the Lee gate."

Once motorists clear the NCIC checks, they will be issued temporary passes. Those who are flagged will be denied access or apprehended if there are outstanding warrants.

At either of the gates, the checks are expected to be short in duration, DeWitt said. "Once we have your ID card, we can have you in and out with a temporary pass within 10 minutes max," he said. It may take a little longer if there is a line, he added.

DeWitt said efforts are also underway to starting running background checks on non-DOD cardholders who currently work on post before the new measures go into effect. Those workers will be issued long-term access passes, provided they have a clear background check.

"By vetting those contractors, subcontractors and others who aren't eligible for a CAC in advance, we will be able to reduce the initial traffic volume at the VCC when it opens," DeWitt said.

In terms of volume, DeWitt said there is no data yet on how many non-DOD ID cardholder motorists enter the installation every day, but that will change soon. "For two-week periods over the next three months, we'll be conducting 100-percent ID checks on everyone entering the installation to assess that number," he said. The Trusted Traveler program, which allows for certain DOD ID cardholders to vouch for passengers in their vehicle, will be temporarily suspended during these times.

DES is currently engaged in an effort to inform all motorists about the pending changes. DeWitt said it is important for everyone to understand that increased security has a price.

"We will be safer," he said of the new policies. "We can rest assured that those who desire to enter Fort Lee are not those who may jeopardize the safety and security of those who live and work here."

NCIC was designed to complement efforts to apprehend fugitives, locate missing persons, recover stolen property and identify terrorists.

Other installations across the Army have already implemented the use of the NCIS database. At Fort Campbell, Ky., for example, 344 people were denied entry for various drug crimes and 36 were turned away for sex offenses in the last quarter of fiscal 2014.

DeWitt added that while derogatory information discovered during background checks can lead to denial of post access, those people are entitled to file an appeal to preserve their access privilege. "Appeals will be addressed on a case-by-case basis," he said.

More details on the background checks and appeals process are forthcoming and will be addressed in an upcoming Traveller issue.

For more information, call the Provost Marshal Office Physical Security Branch at (804) 734-7438.