

DEPARTMENT OF THE ARMY  
HEADQUARTERS UNITED STATES ARMY MANEUVER CENTER OF EXCELLENCE  
1 KARKER STREET  
FORT BENNING, GEORGIA 31905-5000

MCoE Regulation Number 190-13

10 December 2014

INSTALLATION ACCESS CONTROL

**Summary.** This regulation prescribes policies and procedures for granting access to Fort Benning, Georgia. For the purposes of this regulation, the words 'Fort Benning' shall include the installation of Fort Benning, Camp Merrill, and the Morale, Welfare, and Recreation Destin Army Recreation Area. Access control restricts, and/or controls entrance to Fort Benning to only those authorized persons and their vehicles. Persons authorized access will be either escorted or unescorted.

**Applicability.** This regulation applies to all Service members, Family members, federal employees, Civilians and foreign nationals visiting or conducting official business on Fort Benning.

**Punitive nature material.** This regulation is punitive in nature. Individuals who are subject to the Uniform Code of Military Justice (UCMJ) who violate this regulation are subject to administrative or judicial action under the UCMJ. Individuals not subject to the UCMJ are subject to administrative or judicial actions in accordance with applicable federal, state, and local laws or regulations.

**Availability.** This publication is available on the MCoE Administrative Publications SharePoint site @ <https://benna0shrpt2/sites/pubs/default.aspx>

**Effective Date:** The effective date of this regulation is upon signature of the installation commander or his designee.

*Contents*

|  |           |                       |
|--|-----------|-----------------------|
| <b>Chapter 1</b>                                 |           |                       |
| <b>Introduction</b>                              |           | <i>Paragraph Page</i> |
| Purpose .....                                    | 1-1.....  | 1                     |
| References .....                                 | 1-2.....  | 1                     |
| Explanation of abbreviations and terms.....      | 1-3.....  | 1                     |
| Administrative Control.....                      | 1-4.....  | 1                     |
| <br><b>Chapter 2</b>                             |           |                       |
| <b>Installation Access Policy</b>                |           |                       |
| General.....                                     | 2-1.....  | 1                     |
| <br><b>Chapter 3</b>                             |           |                       |
| <b>Access Control procedures</b>                 |           |                       |
| Screening and Vetting.....                       | 3-1.....  | 1                     |
| Authorized Unescorted Access .....               | 3-2.....  | 2                     |
| Trusted Traveler Program .....                   | 3-3.....  | 2                     |
| Uncleared (Non-CAC) Contractors and Vendors..... | 3-4.....  | 3                     |
| Uncleared (Non CAC) Visitors .....               | 3-5.....  | 3                     |
| Fitness Determination .....                      | 3-6.....  | 4                     |
| Access Denial Waiver Application Packet .....    | 3-7.....  | 4                     |
| Approval Process for Denial Waivers .....        | 3-8.....  | 4                     |
| Escorted Access .....                            | 3-9.....  | 5                     |
| Compliance Reporting .....                       | 3-10..... | 5                     |
| <br><b>Chapter 4</b>                             |           |                       |
| <b>Credentialing</b>                             |           |                       |
| Credentialing Categories .....                   | 4-1.....  | 5                     |
| Special Events .....                             | 4-2.....  | 5                     |
| Special Categories .....                         | 4-3.....  | 6                     |

**Chapter 5****CAC Issuance to Contractors (IAW OPOD 15-031)**

|  |          |       |
|--|----------|-------|
| Garrison Security Office Role.....   | 5-1..... | 6     |
| Background Investigation Procedure .....   | 5-2..... | 7     |
| Definitions .....  | 5-3..... | 7     |
| Appendix A - Designation to Determine Fitness for Installation Access .....                                      |          | 10    |
| Appendix B - Installation Access Denial .....  |          | 11-12 |
| Appendix C - Fort Benning Access Control Denial Waiver Application.....  |          | 13-14 |
| Appendix D - Fort Benning Access Request Form .....  |          | 15    |
| Appendix E - Visitor Access Request Form .....   |          | 16    |
| Appendix F - Graduation Letter for Parent .....  |          | 17-18 |
| Appendix G - Retrieval of Common Access Card (CAC) from Contractors at Expiration of Contract or Termination ... |          | 19-21 |
| Appendix H - Industrial Security Program .....   |          | 22-27 |
| Appendix I - CAC Credentialing Flow Chart .....  |          | 28    |
| Appendix J - NCIC III Request Cover Sheet .....  |          | 29    |
| Appendix K - ID Card Request .....   |          | 30    |
| Appendix L - NCIC III request Roster .....   |          | 31-32 |

## Chapter 1 Introduction

### 1-1. Purpose.

This regulation establishes policies, responsibilities and procedures for granting access to Fort Benning.

### 1-2. References.

Required and related publications and prescribed and referenced forms are listed in Appendix A.

### 1-3. Explanation of abbreviations and terms.

Abbreviations and special terms are explained in the glossary.

### 1-4. Administrative Control.

The Directorate of Emergency Services (DES) is responsible for the management and control of installation access. Installation Directorates and Commands are responsible for notifying DES of revoked CAC privileges when CAC cards are not retrieved. The Directorates, Commands, and Agencies are responsible for identifying and notifying DES of their Government Employee Sponsors (GES).

## Installation Access Policy

### 2-1. General.

a. **Scope.** To standardize access control requirements for entering Fort Benning, Georgia relating to vehicle and personnel screening, identification (ID) documents, vehicle registration, long term access control card and temporary passes.

b. **Authority.** Authority to control access to United States Army Installations varies based on jurisdiction, property rights, and Geographic location. Within US jurisdiction, commanders publish and enforce guidance to protect installation resources in accordance with (IAW) Department of Defense (DoD) and Army policy. DoD Instruction (DoDI) 5200.08, Security of DoD Installations and Resources and DoD Physical Security Review Board, prohibit individuals from entering military installations within the jurisdiction of the U.S. for a purpose prohibited by law or lawful regulation, or reentering an installation after being ordered not to reenter by an officer in command of the installation.

c. **Policy.** IAW Army Directive 2014-05 All personnel desiring unescorted access to Army installations will enter the installation through an authorized Access Control Point (ACP) and be vetted using the National Crime Information Center (NCIC) Interstate Identification Index (III). Security personnel will validate persons that have a valid reason to be on the installation. Security personnel will verify the identification of all persons entering Fort Benning through the installation's Visitor Control Centers (VCC) and ACPs IAW the references in appendix A.

d. Individuals who disrupt, impede, interfere, or assault Department of the Army Security Guards (DASG) or other security personnel in the performance of ACP operations will be detained by DASGs. Law Enforcement personnel will return these individuals to the Military Police Station for processing. Individuals may be titled under the UCMJ or Title 18, Sec 111, USC.

## Chapter 3 Access Control Procedures

### 3-1. Screening and Vetting.

a. **Screening (Identity Proofing).** Security personnel performing installation access control will verify a person's need to have access to the installation and perform a physical (touch) and visual inspection on all identifications of occupants. The inspection will include:

1. Visual match of the photograph on the card to the person presenting the ID.
2. Verifying authenticity by checking the anti-counterfeit or fraud protection embedded in the credential.
3. Authenticating cards using automated means at installations where physical access control systems (PACS), such as Automated Installation Entry (AIE), have been fielded.

#### b. Vetting.

1. **NCIC III.** A check of records through the National Crime Information Center (NCIC) Interstate Identification Index (III) is the Army baseline background check for entrance onto Army installations for Non-Common Access Card (CAC) holders to include visitors. The FBI permits the use of NCIC III for vetting of visitors to ensure the security of military installations.

2. **ID Requirements.** All persons age 18 and over must present a valid picture identification card for access to the installation. Personnel under the age of 18 will not have a NCIC-III check conducted.

a) **Vehicle occupants** who are 18 years of age or older must be in possession of a valid picture identification card (for example, drivers license, state identification, DD Form 1173 (Uniformed Services Identification and Privilege Card), DD Form 2 series, passport) issued by an authoritative agency (state/federal) so they can be readily identified while on the installation.

b) Occupants below the age of 18 who do not possess a valid picture identification card may be vouched for by an adult occupant of the vehicle who has been cleared to enter the installation.

c. ID Documents. DoD CAC per DoDI 8190.3 is the standard identification card for Active and Reserve uniformed personnel, DoD Civilian employees, eligible contractors and some designated foreign nationals. The CAC shall be the principal access control card which enables access to buildings, facilities, installations, and some limited controlled spaces.

d. Unescorted access will not be granted without completing a favorable NCIC-III screening.

e. Escorted Personnel.

1. Non-DoD affiliated personnel who have not been vetted through the NCIC will be escorted while on the installation.

2. The escorted person must present a valid state driver's license, state identification card with photo, a valid U.S. passport, or a valid passport from other countries cleared by the State Department.

3. Only those personnel who have been granted unescorted access without a NCIC-III checks are authorized to escort Non-DoD affiliated personnel.

### 3-2. Authorized Unescorted Access

a. Personnel in lawful possession of a valid form of the following identification credentials are authorized unescorted access onto the installation.

1. DoD CAC

2. DoD Form 2 and DD 1173. The Uniformed Services Identification and Privileges Card are issued to military dependents and retirees.

3. DA Form 1602, Civilian Identification Card

4. DD Form 489, Geneva Convention Identification card for medical and religious personnel.

5. DD Form 2574, Armed Forces Exchange Services identification and privilege card.

6. DD Form 2764, US DoD/Uniformed Services Civilian Geneva Convention Identification.

7. Air Force (AF) Form 354, civilian identification card.

8. Gold Star Installation Access Card after a favorable NCIC-III background check.

9. Automated Installation Entry (AIE) pass or card. The pass or card is a valid installation access credential for individuals who do not otherwise meet requirements for a CAC. The AIE pass or card is issued at the VCC to individuals who have a valid reason to access the installation and successfully pass a NCIC III check.

10. Local, state, and federal government agencies including members of Congress, their staff representatives and elected public officials with official picture identification cards and or credentials will be granted access to the installation.

11. Local, state and federal law enforcement, Fire and EMS officials driving official or emergency vehicles or privately owned vehicles whether armed or unarmed must present their credentials. Fort Benning Law Enforcement, Fire, EMS and requested emergency responders on an active emergency response are not required to show identification. Prior notice to Access Control Points will be made through Fort Benning emergency dispatchers.

b. Unescorted Access - Personnel requiring an Automated Installation Entry (AIE) card because they do not qualify for a CAC card will request a card through their Government Employee Sponsor (GES). GES will provide the request through DES VCC to obtain the AIE Card. The request will be processed through the NCIC III and be vetted against disqualifying criteria found in IMCOM OPOD 15-031. Personnel who pass NCIC III vetting will be notified through their GES of the time, date and location to report to an AIE station for issuance of a card.

c. Responsibility of the GES.

1. GES ensure the personnel they request unescorted access for have a valid need to enter post.

2. The GES is the government representative who conducts the initial assessment of a person's need for access and fitness to be granted access in accordance with IMCOM OPOD 15-031 and this policy.

3. The GES will be informed by agencies on the installation of any violations of law, policy or regulations by the personnel they sponsor.

4. The GES may request revocation of a sponsored person's access privileges based on the information available to them.

5. The GES is the first appeal authority for sponsored persons receiving a denial of access privilege.

### 3-3. Trusted Traveler Program (TTP)

a. The TTP may be initiated by the Installation Commander upon the commissioning of an AIE system. The Installation Commander at his discretion may suspend the TTP based on local threat or may revoke individual trusted traveler privileges. The TTP allows persons 18 years or older and are uniformed service members and spouses, DoD employees, CAC Contractors, and retired uniformed service members and spouses to vouch for occupants in their immediate vehicle, provided the Trusted Traveler vehicle operator possess a valid identification card and has a clear NCIC III check. The intent of the TTP is to-

1. Expedite access to the installation for uniformed service members and spouses, DoD employees, and retired uniformed service members and spouses.

2. Provide a high degree of security with faster vehicle throughput.

3. Mitigate traffic congestion on adjoining highways.

4. Provide for flexibility for trusted travelers to vouch for family members and official visitors.
  - b. The TTP is not authorized for military dependents (except spouses), non-CAC contractors, volunteers, or family care providers.
  - c. The TTP does not authorize vehicle occupants to enter a MEVA, defense critical asset, task critical asset, or limited area, or exclusion area without first meeting the security requirements and procedures for those areas.
  - d. Trusted travelers are responsible for the actions of all occupants in their vehicle and for meeting all local security requirements for escort as established by Army Regulations and requirements of the Installation Commander.
  - e. Trusted travelers cannot vouch for persons with foreign passports or identification cards who must, instead, be cleared per AR 190-13 paragraph 8-2.
  - f. The TTP will be suspended at FPCON Charlie and Delta and the Installation Area Access Control Plan will reflect procedures when TTP is suspended.
  - g. Persons registering for trusted traveler status will register at designated registration locations. The trusted traveler token will be registered into the AIE database. TTP is a local installation program and not recognized at other installations.

#### 3-4. Uncleared (Non-CAC) Contractors and Vendors (Contractor Access to Fort Benning)

- a. All contractors requiring unescorted access to the installation on a recurring basis for a period of 6 months or more, shall receive a CAC. CACs are issued through the Contractor Verification System (CVS) program. Issuance of a CAC requires a favorable FBI fingerprint check, successful submission of a National Agency Check with Inquiries (NACI)(equivalent of higher) background investigation to the Army's investigative service provider and a favorably adjudicated NACI (equivalent or higher) investigation from a federal department or agency will be accepted. To avoid delays in gaining required access to the installation, all contractors eligible for a CAC are encouraged to contact their Contracting Officer Representative (COR) to begin the process to obtain CACs as soon as possible.
- b. Contractors and vendors requiring physical access to the installation longer than 24 hours and less than 6 months but do not require access to a DoD computer network are not eligible for a CAC. Non-CAC eligible contractors who have a contractual agreement will have a government employee sponsor provide the contractual agreement with a cover memorandum signed by a verifying officer vouching for the need to possess an AIE card to the VCC. The expiration date of the AIE card will be the end date of the contract or visit, or the expiration of the sponsor's credential, whichever comes first. Sub-contractors will be bound by the same requirement.
- c. Military ID cards for retirees, reservists and dependents is for non contractor use. All contractors and sub contractors possessing a valid Military ID and requiring access to the installation for contractor related reasons will comply with paragraph 3-5a or 3-5b.
- d. All contractors and sub contractors who do not possess a CAC and do not meet the requirements of paragraph 3-5a to c will report to the VCC with valid federal or state picture identification to be issued a temporary pass. A temporary pass will only be issued to persons with a valid reason for unescorted access who successfully pass a check of NCIC III and the post exclusion roster.

#### 3-5. Uncleared (Non-CAC) Visitors

- a. All Non CAC / Military ID holders with a valid reason to require unescorted access to the installation will report to the VCC with a valid Federal or state picture identification to be issued a temporary pass. A temporary pass will only be issued to persons with a valid reason for unescorted access and pass a check of NCIC III and the post exclusion roster.
- b. Non CAC / Military ID holders may be escorted by a DoD sponsor. The DoD sponsor must meet the criteria of paragraph 3-4a above with caveat. The Non CAC / Military holder will be physically escorted by the DoD sponsor at all times while on the installation. The DoD sponsor is responsible for all actions of the sponsored Non CAC / Military holder while on the installation.
- c. Special Events. A NCIC III screening for personnel attending special events and activities may be waived where screening is impractical. Compensatory security measures for special events will be implemented for non DoD credentialed individuals without a DoD sponsor escort. For large special events (for example, football games, 4<sup>th</sup> of July, graduations, concerts) non-DoD credentialed visitors without a DoD sponsor escort will be directed to enter the installation through the identified special event gates where security measures are conducted prior to entrance onto the installation. Non installation level special events (for example, weddings, reunions, unit functions) the DoD sponsor will provide a special event access attendee list to the VCC prior to the event. Non DoD credentialed visitors without a DoD sponsor escort attending the event will be directed to a specific ACP where they will be vetted against the special event access list for that particular special event.
- d. Graduations visitors that are not in possession of an invitation letter will be vetted against the graduating class roster. The

Military ID holder will be designated as the GES for the duration of the visit. Additional screening measures will be used to validate fitness for entry.

### 3-6. Fitness Determination. (See Appendix A-1).

a. Unescorted Access Determination. The Installation Commander will, in the absence of an approved waiver deny un-cleared contractors, subcontractors and visitors unescorted access to the installation based on the results of the NCIC III check that contains credible derogatory information indicating the individual may present a threat to good order, discipline, or health and safety on the installation. Such derogatory information includes, but is not limited to the following:

1. The NCIC III contains criminal arrest information about the individual that causes the Installation Commander to determine that individual presents a potential threat to the good order, discipline, or health and safety on the installation.
2. The installation is unable to verify the individual's claimed identity based on the reasonable belief that the individual has submitted fraudulent information concerning his or her identity in the attempt to gain access.
3. The individual has a current arrest warrant in NCIC, regardless of the offense or violation.
4. The individual is currently barred from entry or access to a federal installation of facility.
5. The individual has been convicted of crimes encompassing sexual assault, armed robbery, rape, child molestation, production or possession of child pornography trafficking in humans, drug possession with the intent to sell or drug distribution.
6. The individual has a US conviction for espionage, sabotage, treason, terrorism or murder.
7. The individual is a registered sex offender.
8. The individual has a felony conviction within the past 10 years, regardless of the offense or violation.
9. The individual has been convicted of a felony firearms or explosives violation.
10. The individual has engaged in acts or activities designed to overthrow the U.S. Government by force.
11. The individual is identified in the Terrorist Screening Database (TSDB) as known to be or suspected of being a terrorist or belonging to an organization with known links to terrorism or support of terrorist activity.
12. Individuals barred from Fort Benning.

b. Access Denial Waiver Process. In cases where an un-cleared contractor, subcontractor or visitor is denied access based on derogatory information obtained from an NCIC or NCIC III check, the Installation Commander will offer the following process only if the individual requests a waiver.

c. Personnel at the ACP or VCC will issue the denied individual instructions on how and where to submit a waiver.

### 3-7 Access Denial Wavier Application Packet.

- a. The access denial wavier application packet will instruct the individual to do the following:
1. Obtain a certified copy of their complete criminal history, which must include all arrests and convictions.
  2. Complete an Installation Access Control Denial Waiver Application and provide the packet to the government sponsor, who will be responsible for submission of the waiver application to the Installation Commander. All offenses must be listed, along with providing an explanation why the conduct should not result in denial from entering the Army installation. Other factors that should be addressed by the sponsor/applicant are:
    - a) Nature and seriousness of the conduct
    - b) Specific circumstances surrounding the conduct
    - c) Length of time elapsed since the conduct
    - d) The age of the individual at the time of the incident/conduct
    - e) Proof of efforts towards rehabilitation
  3. Provide a current physical or e-mail address to enable the Senior Commander to transmit a copy of his/her waiver request determination.
    - a) The government sponsor will review the individual's packet for completeness and determine whether or not to endorse the waiver.
    - b) If the government sponsor determines to endorse the waiver, he/she must provide a letter. The letter must indicate that the sponsor requests that the individual be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visits.
    - c) If a contractor employee is terminated, the sponsor must inform the Senior Commander so that unescorted access to the installation is no longer authorized.

### 3-8. Approval Process for Denied Waivers.

- a. The designated government official(s) will review the access denial wavier applications and make a fitness determination recommendation to the approving authority. Unless otherwise delegated down, the Installation Commander is the approving authority.
- b. The Installation Commander or delegated official will review the waiver application and render a determination that ensures proper protection of good order and discipline, or health and safety on the installation.
- c. The Senior Commander or delegated official will provide a copy of the determination to the individual, and to the Director of Emergency Services/Provost Marshal Office and sponsoring agent.

d. Individuals who have had a waiver request denied may request reconsideration from the Senior Commander after one year from the date of the commander's decision, or earlier if the individual can present significant information that was not available at the time of the original request or that the basis for the original denial was overturned, rescinded or expired.

### 3-9. Escorted Access.

a. DoD personnel in possession of approved forms of ID (ex: MIL ID, CAC) may escort personnel on post. The personnel being escorted do NOT require an NCIC check and are NOT required to report to the Visitor Control Center (VCC). Escort personnel are entirely responsible for the actions of all occupants in their vehicle and for meeting all local security requirements for escort as established by Army Regulations and requirement of the installation commander.

b. Responsibility of the DoD personnel providing escort to un-vetted personnel. Escorts will ensure their guest(s) follows laws, regulations and policy while on post. The escort will ensure all guests depart the installation. The escort will immediately report violations of their guests to the Provost Marshal's Office. Escorts may be held accountable for negligent execution of these duties.

### 3-10. Compliance Reporting.

DPTMS will submit IMCOM Installation Access Compliance Reports on the first day of each month IAW OPOD 15-031, Annex C.

## Chapter 4 Credentialing

### 4-1. Credentialing Categories.

a. Installation Commander will use locally produced installation badges and temporary passes for all Non-DoD affiliated people gaining access to the installation.

1. The local identification badge will be a DBIDS, DBIDS-like card with an imprinted photo and expiration date. Local badges should be issued to personnel who will need regular access to the installation for a period of 30 days or longer and not to exceed one year.

2. The local passes, better referred to as vehicle passes, will have the expiration date fully visible and be issued for short term installation access. The local pass should be issued to those individuals who only need access to the installation for a period of 30 days or less.

b. Personnel in lawful possession of a valid form of the following identification credentials are authorized unescorted access onto Army installations without needing a NCIC- III check conducted:

1. DOD CAC
2. DD Form 2A (ACT) (Active Duty Military Identification Card)
3. DD Form 2 (ACT/RES) (Armed Forces of the United States-Geneva Conventions Identification Card (Active and Reserve)
4. DD Form 2 (RET) (United States Uniformed Identification Card (Retired)
5. DD Form 2S (ACT/RES) (Armed Forces of the United States-Geneva Conventions Identification Card (Active and Reserve)
6. DD Form 2S (RET/RES RET) (United States Uniformed Identification Card (Retired and Reserve Retired)
7. United States Government issued authenticated Federal PIV credentials.

c. Personnel in lawful possession of a valid form of the following identification credentials are authorized unescorted access onto Army installations after a favorable NCIC- III check is conducted:

1. State valid driver's license
2. Locally issued installation badge and/or pass
3. DA Form 1602 (Civilian Identification and Gold Star Family)
4. School District Employees ID (only until the installation has a local produced badge)
5. The Transportation Security Agency (TSA) issued Transportation Worker Identification Credential (TWIG)
6. DD Form 2574, Armed Forces Exchange Services ID and Privilege
7. Air Force (AF) Form 354, Civilian ID
8. DD Form 1934, Geneva Convention ID card for Medical and Religious
9. DD Form 2764, US DoD/Uniformed Services Civilian Geneva Convention ID
10. DD Form 489, Geneva Convention ID card for Civilians

d. Official foreign visitors (e.g., Foreign Liaison Officer, Foreign Exchange Personnel, and Cooperative Program Personnel) subject to the provisions of AR 380-10 will be granted unescorted visitor status. The Foreign Visit System-Confirmation Module will be used to confirm that a proposed official visit to an Army installation by a foreign government representative has been approved through the Foreign Visits System, and to record the arrival of such visitors.

### 4-2. Special Events.

a. Senior Commanders may continue to grant waivers for special events IAW AR 190-13, Para 8-6.

b. A risk analysis will be accomplished to assist in developing compensatory security measures when NCIC-III screening is impractical and regulatory requirements cannot be met. The following are examples to be considered when planning the event:

1. Isolate event traffic and parking to specific locations.
2. Transport attendees to and from the event utilizing government transportation.
3. Direct event traffic to specific ACPs where security measures are conducted prior to attending the event.

#### 4-3. Special Categories.

##### a. Commercial Delivery Vehicles

1. Drivers must possess a current bill of lading for the specific delivery containing an address on the installation.
2. Drivers must possess a valid state issued DL, state vehicle registration, and proof of insurance.
3. All delivery vehicles may be subject to a vehicle inspection.
4. Unless escorted, drivers will be cleared through NCIC-III prior to making the delivery.
5. If the vehicle has a seal, the seal's serial number will be checked against the bill of lading to ensure the cargo has not been tampered with. If the seal is broken or the serial number does not match, a 100% inspection of the vehicle will be conducted.

##### b. Food Deliveries / Vendors

1. Vendors and drivers must apply for a visitor pass and be cleared through NCIC-III.
2. Drivers must possess a valid state issued DL, state vehicle registration and proof of insurance.
3. All vehicles are subject to inspection prior to being granted access.
4. Deliveries must have an on-post destination.
5. Installation Commander will determine if a food delivery or vendor drivers are issued an installation badge or pass.

##### c. Taxis

1. Taxi drivers must apply for a visitor pass and be cleared by NCIC-III.
2. Drivers must possess a valid DL, valid taxicab operator's "hack" license, vehicle registration, and proof of insurance.
3. Vehicles are subject to be inspected before access is granted.
4. Taxis drivers will not be granted trusted traveler status.
5. Installation Commander will determine if a taxi driver is issued an installation badge or pass.

##### d. Tow Trucks

1. Tow truck drivers must apply for a visitor pass and be cleared by NCIC-III.
2. Drivers must possess a valid tow tag, tow truck certificate of registration, tow truck application, cab-card, valid DL, state vehicle registration, and proof of insurance.
3. Vehicles are subject to be inspected before access is granted.
4. Tow truck drivers will not be granted trusted traveler status.
5. Vehicles being towed for maintenance reasons will be verified telephonically with the person(s) requesting the tow.

##### e. Repossessions

1. Creditors, or their agents, requesting access to recover property based on default of a contract or legal agreement are required to coordinate through the Provost Marshal Office/ DES.
2. The Police Desk will provide an escort and notify the Installation Staff Judge Advocate (SJA).
3. The creditor or their agent must adhere to the following procedures:
  - a) Copy of title, contract or legal agreement must be presented.
  - b) Present evidence that the debtor is in default of the contract or legal agreement.
  - c) Agents must present evidence they are working for the creditor.

##### f. Movers

1. Drivers must possess a current bill of lading for the specific delivery containing an address on the installation.
2. Drivers must possess a valid state issued DL, state vehicle registration, and proof of insurance.
3. All delivery vehicles may be subject to a vehicle inspection.

##### g. Gold Star Family Procedures (DA Form 1602)

1. Ensure that the NCIC-III check is conducted prior to issuance.
2. Coordinate with the SOS Office and ensure the date of the NCIC-III check is typed onto the DA Form 1602.
3. Annotate within local policy if the installation accepts the Gold Star Family Member ID from other installations.

#### Chapter 5

#### CAC Issuance to Contractors (IAW OPOD 15-031)

##### 5-1. FBGA Garrison Security Office Role

a. This chapter is intended as a guide to define the role of the FBGA Garrison Security Office (GSO) in processing U.S and Foreign National contractors who are authorized and require CAC-eligible access to government installations and facilities. Security Officers and Servicing Agencies must become familiar with Army Directive 2014-05 dated 7 March 2014 and references for detailed guidance on applying any applicable processes.

b. The DPTMS GSO supports HSPD-12 by requesting, tracking, receiving and interpreting appropriate investigations required in order to issue contracted employees (contractors) Common Access Cards (CAC).

c. The GSO accomplishes this by processing requests from the sponsoring activity or COR to verify the contractor's investigation

status for CAC issuance. The Sponsoring Activity is responsible for determining if an employed contractor is CAC-eligible or non-CAC eligible. It is not the responsibility of the security office to determine access eligibility. Once the COR identifies CAC-eligible contractors to the GSO, the GSO will execute the investigation process required for CAC issuance. Any questions regarding the individual's eligibility will be directed to the Sponsoring Organization's COR.

d. Other offices involved in the HSPD-12 process include:

1. The Trusted Agent (TA)/ Trusted Agent Security Manager (TASM) who operates the Trusted Associate Sponsorship System (TASS). The TA/TASM is responsible for verifying a contractor's investigation in TASS for CAC issuance and will coordinate with the GSO regarding the status of an investigation or continued eligibility of a contractor. Continued eligibility of a contractor will depend upon information that becomes available as a result of the investigation.

2. The Installation ID Card section of the Military Personnel Division (MPD), which normally issues the CAC.

3. The Directorate of Emergency Services, which directs the mission of the physical access to installations.

e. The GSO will execute the investigation process only upon request from the Sponsoring Agency or COR. The GSO will initiate and track the investigation until the results are received. The GSO will provide the investigation results to the Sponsoring Agency or COR for a determination. If requested, the GSO will provide an interpretation of the results to the requestor.

f. In the case of adverse results, in which the subject contractor's investigation is not adjudicated favorably, the Sponsoring Activity's appointed official will receive and process correspondence from DOHA and notify the subject contractor in writing. The appointed official is responsible for guiding the individual through the appeals process for reconsideration. The GSO will advise as necessary during these actions.

## 5-2. Background Investigation Procedure.

a. Initial (Interim) issuance of a CAC requires the following:

1. Completion of a Federal Bureau of Investigation (FBI) fingerprint check with favorable results;

2. Favorable review of the contractor's eQIP (SF 85/SF 86) by the servicing security office.

3. Upon the successful submission of a National Agency Check with Inquiries (NACI) (equivalent or higher) investigation through the U.S. Army Personnel Security Investigation Center of Excellence (PSI CoE) to the U.S. Office of Personnel Management (OPM) (the Army's investigative service provider).

4. Verification that OPM has opened the individual's investigation.

5. Or verification of an already current investigation on file that meets or exceeds the criteria required by HSPD-12 policy.

b. The COR is the deciding authority regarding initial (interim) CAC issuance in the case where the investigation is not yet complete on a contractor.

c. A final CAC determination requires a favorably adjudicated NACI (equivalent or higher) investigation based on the basic and supplemental HSPD-12 credentialing standards. Sponsoring activity CORs are the determining official as to the final issuance of a CAC card to contracted employees. CORs will coordinate final decisions with the sponsoring command leadership.

d. Credentialing of Non-U.S. Nationals. Whether located OCONUS or CONUS, sponsoring activities are required to apply the same CAC credentialing process and adjudication standards to non-U.S. national contractor employees who are eligible for a CAC in accordance with AD 2014-05. GSOs are responsible to coordinate and understand processes involving host nation investigation equivalents.

e. System of Record.

1. The GSO will ensure all final credentialing determinations are annotated in the DoD Case Adjudication Tracking System (CATS) portal, which transmits a record of the determination to the OPM Central Verification System (CVS). The OPM CVS is the system of record for recording final determinations on CAC credentialing.

2. The COR is responsible to communicate any information (derogatory) to the GSO if it may have an effect on the credentialing status of a contractor.

f. IMCOM GSOs will submit background investigations or screening requests for all contract employees under contracts initiated by FBGA elements or sponsored by an IMCOM element. The FBGA GSO at an installation will support tenant units as they currently do (status quo). If a tenant requires HSPD-12 support from the GSO, the GSO will attempt to accommodate the tenant's needs. However, when executing the HSPD-12 (CAC-eligible) investigation responsibilities for a tenant, the GSO will abide by the same procedures and constraints directed by this Regulation or other formal IMCOM policy or direction.

## 5-3. Definitions.

a. A CAC-eligible contractor is defined as any U.S or Foreign National contractor who is authorized and requires access to multiple (2 or more) DoD-controlled installations or facilities on behalf of the Department of the Army on a recurring basis for a period of 6 months or more; or requiring both access to a DoD controlled installation or facility and onsite or remote access to DoD or Army controlled information networks.

b. The practical application of the term "facility", with respect to HSPD-12 CAC-eligible determination is as follows:

1. Separate buildings located on an installation that do not employ special security measures are not considered facilities separate from the installation.

2. Buildings or activities where special security measures (i.e. Controlled Access Areas) are employed may be considered a separate "facility" from the installation, in accordance with the determination of the command leadership of the particular building activity.

3. Buildings or offices not located on an Army installation (i.e. leased buildings) are considered separate facilities. Depending upon their level of security measures, a contractor may require a CAC in order to access even one facility of this category.

c. In accordance with these definitions, generally, a contractor who needs access to an installation, with no access to buildings with special security (such as a SCIF or research facility) is deemed to only be accessing a single facility.

d. A contractor who requires access to two separate installations that are not geographically co-located, or two installations that are separated by a layer of security (i.e. JBLM), is deemed to be accessing two "facilities."

e. A contractor may become CAC-eligible if he/she accesses an Installation and a facility on that installation that employs special security measures.

**References**

**Section I**

**Required and related publications**

- Homeland Security Presidential Directive – 12
- DTM 09-012
- DTM 14-005
- Army Directive 2014-05
- AR 190-13 Chapter 8
- IMCOM OPORD 15-031
- Gold Star Installation Access IMCOM Memorandum

**Section II**

**Referenced Forms**

- FB (DES) Installation Access Form
- Installation Access Denial Memorandum
- Fort Benning Access Control Waiver Denial Application

**Glossary**

**Section I**

**Abbreviations**

- AA&E ..... Arms, Ammunition, and Explosives
- AR ..... Army Regulation
- AAFES ..... Army, Air Force Exchange Service
- GES... ..... Government Employee Sponsor
- AIE ..... Automated Installation Entry
- NCIC-II..... National Crime Information Center Interstate Information Index
- VCC..... Visitor Control Center
- RAPID ..... Gate RCX

**FOR THE COMMANDER:**

MICHAIL S. HUERTER  
COL, IN  
Garrison Commander

  
JAMES E. BRINSON

Director of Human Resources

**DISTRIBUTION:**

- A
- 3 – Publications Management (IMBE-HRA)

## Appendix A – Designation to Determine Fitness for Installation Access



DEPARTMENT OF THE ARMY  
US ARMY INSTALLATION MANAGEMENT COMMAND  
ATLANTIC REGION  
GARRISON COMMAND  
1 KARKER STREET, BUILDING 4, SUITE 5900  
FORT BENNING, GEORGIA 31905-5000

IMBE-Z

05 December 2014

MEMORANDUM FOR Directorate of Emergency Services, Fort Benning, Georgia

SUBJECT: Designation to Determine Fitness for Installation Access

1. In accordance with the provisions of enclosure 2, Army Directive 2014-05, Adjudication Standards and Procedures for Using the National Crime Information Center and Terrorist Screening Database for Installation Access Control of Unescorted, Uncleared Contractors, I hereby designate the authority to determine fitness for installation access to Fort Benning, Georgia to the following duty positions:
  - a. Chief of Police, Access Denial Authority.
  - b. Directorate of Emergency Services (DES), Police Division Branch Chiefs, Access Denial Authority.
  - c. DES, Department of the Army Security Guard (DASG) Supervisors, Access Denial Authority.
  - d. DES, DASG Leads, Access Denial Authority.
  - e. MP Duty Officers, Access Denial Authority.
  - f. MP Patrol Supervisors, Access Denial Authority.
  - g. MP Desk Sergeants, Access Denial Authority.
2. I retain authority to cancel or withdraw this delegated authority at any time. This delegation is subject to review by the new commander upon my change of command.
3. This delegation has been coordinated with the Fort Benning Staff Judge Advocate who concurs with my action. The point of contact is Mr. Dick Gordon, Office of the Staff Judge Advocate, Chief Administrative and Civil Law, at (706) 545-1130.

A handwritten signature in black ink, appearing to read "Michail S. Huarter".

MICHAIL S. HUERTER  
COL, IN  
Garrison Commander

## Appendix B – Installation Access Denial



DEPARTMENT OF THE ARMY  
 US ARMY INSTALLATION MANAGEMENT COMMAND  
 ATLANTIC REGION  
 GARRISON COMMAND  
 1 KARKER STREET, BUILDING 4, SUITE 6900  
 FORT BENNING, GEORGIA 31905-6000

REPLY TO  
 ATTENTION OF

IMBE-Z

05 December 2014

MEMORANDUM FOR \_\_\_\_\_

SUBJECT: Installation Access Denial

1. You are hereby denied access to the Fort Benning Military Reservation because of conduct detrimental to good order and discipline and the performance of the military mission of this installation.

2. In accordance with Army Directive 2014-05 your exclusion from Fort Benning is for the following reason (s):

\_\_\_\_\_

\_\_\_\_\_

3. The offense(s) in paragraph 2, above, warrant permanent exclusion from Fort Benning. However, prior to a decision being made regarding your permanent exclusion from Fort Benning, you have the opportunity to rebut the allegations contained in paragraph 2 and present any evidence in your behalf to submit a waiver. Your rebuttal must contain the following documents:

a. Obtain a certified copy of your complete criminal history, which must include all arrests and convictions.

b. Obtain a letter of support from your Government sponsor. The letter must indicate that the sponsor requests that you be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visits. If you are a terminated contractor employee, the sponsor must notify the senior commander and unescorted access is no longer authorized.

c. Complete an Installation Access Control Denial Waiver Application and provide the packet to the Government sponsor. The Government sponsor is responsible for submitting the waiver application to the senior commander. All offenses must be listed, along with an explanation why the conduct should not result in denial of access to the installation. Other factors the sponsor/applicant should address are the:

- 1) Nature and seriousness of the conduct
- 2) Circumstances (in specific) surrounding the conduct
- 3) Length of time elapsed since the conduct
- 4) Age of the individual at the time of the incident or conduct
- 5) Proof of efforts toward rehabilitation

IMBE-Z  
SUBJECT: Installation Access Denial

d. Provide a current physical or email address to enable the senior commander to transmit a copy of his/her determination on the waiver request.

4. This information may be presented in writing to the Commander, U.S. Army Maneuver Center of Excellence Center, ATTN: IMSE-JA (Fort Benning Hearing Officer), Fort Benning, Georgia 31905.

5. Entering the Fort Benning Military Reservation for any reason, other than as described above, after the date of this memorandum will constitute criminal trespass in violation of Section 1382, Title 18, United States Code, and is punishable by a fine of not more than \$5000 or imprisonment for not more than six months, or both.

6. Final action on this matter is delayed pending your reply. If no reply is received within seven working days, you may be permanently excluded from the Fort Benning Military Reservation.



MICHAIL S. HUERTER  
COL, IN  
Garrison Commander

ACKNOWLEDGEMENT:

I acknowledge receipt of the foregoing order of exclusion and understand that unless I contact the Fort Benning Hearing Officer, as described in paragraph 3 above, by \_\_\_\_\_, I may be permanently excluded from Fort Benning.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

FB , 24October2014 (Installation Access Denial)

Denial Memo No. \_\_\_\_\_

## FORT BENNING ACCESS CONTROL DENIAL WAIVER APPLICATION

**WARNING: ANY MISREPRESENTATION OR OMISSION OF INFORMATION MAY RESULT IN DENIAL OF THE REQUEST**

| <b>APPLICATION REQUEST</b>  |   |                                   |   |
|---|---|-----------------------------------|---|
| Please type or print neatly; Attach additional sheets if necessary  |   |                                   |   |
| 1. Name ( <i>First/Middle/Last</i> )  |   |                                   |   |
| 2. Current Address ( <i>Number and Street, City, State, and ZIP Code</i> )  |   |                                   |   |
| 3. Email address:<br>Do you want your decision emailed back to you rather than mailed to you? <input type="checkbox"/> Yes  |   |                                   |   |
| 4. Current Telephone Number<br>Home ( ) - - Work ( ) - -  |   |                                   |   |
| 5. Reason for requesting access to Fort Benning?  |   |                                   |   |
| 6. What job has Fort Benning offered you?   |   |                                   |   |
| 7. Does your job require you to have a clearance?   |   |                                   |   |
| 8. List Your <b>ENTIRE</b> Criminal History ( <i>except traffic and other infractions</i> ) as follows:   |   |                                   |   |
| CRIME FOR WHICH YOU WERE ARRESTED   | CRIME FOR WHICH YOU WERE CONVICTED (OR INDICATE IF DISMISSED OR NULL PROS.) | NAME & ADDRESS OF COURT OR AGENCY | DISPOSITION ( <i>INCLUDE SENTENCE AND CONVICTION DATE</i> ) |
|   |   |                                   |   |
|   |   |                                   |   |
|   |   |                                   |   |
|   |   |                                   |   |
| 9. Attach a copy of all court documents, certified by the Clerk of the Court, from all of your conviction(s).   |   |                                   |   |
| 10. In your own words, explain the facts of each felony, and why you should be able to come on post. Attach additional sheets if necessary.                             |   |                                   |   |
|   |   |                                   |   |
|   |   |                                   |   |
| 11. Explain any circumstances that lessen the seriousness of the felony conviction(s) and show that you have been rehabilitated. Attach additional sheets if necessary. |   |                                   |   |
|   |   |                                   |   |
|   |   |                                   |   |

Appendix C – Fort Bening Access Control Denial Wavier Application

|   |
|---|
|   |
|   |
|   |
|   |
| 12. Have you been denied access by any other federal organization? <i>(please circle)</i><br>Yes            No<br>If yes, indicate the reason for the denial. |
|   |
|   |
|   |
|   |
| 13. List all references that you would like the review officer to consider on your behalf. Include name, address, telephone number, and relationship:         |
|   |
|   |
|   |
|   |
|   |

VERIFICATION

State of \_\_\_\_\_ )

County of \_\_\_\_\_ )

Under the penalty of perjury, the undersigned has examined this request for review and to the best of my knowledge and belief, it is true, complete, and correct.

\_\_\_\_\_  
Your Signature

\_\_\_\_\_  
Your printed name

\_\_\_\_\_  
Date (Month, Day, Year)

Before me, the undersigned, a Notary Public in and for said County and State, personally appeared \_\_\_\_\_ and acknowledged the execution of the foregoing instrument as his/her voluntary act and deed.

WITNESS, my hand and Notarial Seal, this \_\_\_\_ day of \_\_\_\_\_, 20 \_\_\_\_.

\_\_\_\_\_  
Notary Public, Written Signature

Appendix D - Fort Benning Georgia Access Request Form

|  |         |                             |  |   |                             |
|--|---------|-----------------------------|--|---|-----------------------------|
| <b>FORT BENNING GEORGIA ACCESS REQUEST FORM</b><br><small>(THIS FORM IS SUBJECT TO THE PRIVACY ACT OF 1974)</small>  |         |                             |  | CIRCLE ONE: <b>Long-Term Pass</b> <b>Civilian</b> |                             |
| <b>Contractor/Partner</b>  |         |                             |  |   |                             |
| Complete this form and return to your Fort Benning sponsor. A National Crime and Information Center (NCIC) check will be conducted prior to granting access to the installation. By signing this application, you affirm/swear the information provided is true. That a knowing and willful false statement on this application can be punished by barment from the installation, a fine, imprisonment or both. (18 U.S.C. Section 1001). Furthermore, that under the authority of 50 U.S.C. Section 797 and DoD 5200.8, the installation commander has imposed a continuing obligation for you to disclose to Fort Benning, within 24 hours, if you're convicted of any criminal offenses that occur while you have unescorted access authority to Fort Benning   |         |                             |  |   |                             |
| <b>Section I. PERSONAL INFORMATION</b>   |         |                             |  |   |                             |
| 1. NAME (Last, First, Middle)  |         | 2. DRIVER'S LICENSE #/State |  | 3. Social Security Number                         | 4. DATE OF BIRTH (YYYYMMDD) |
| 5. CURRENT ADDRESS (Include City/State/ZIP Code)   |         |                             | 6. HOME PHONE NUMBER   |   | WORK PHONE NUMBER           |
| 7. SEX   | 8. RACE |                             | 9. EYE COLOR   | 10. HAIR COLOR                                    | 11. HEIGHT                  |
| 12. WEIGHT   |         |                             |  |   |                             |
| <b>Section II. PLACE OF BIRTH</b>  |         |                             |  |   |                             |
| 1. CITY  |         | 2. STATE (If applicable)    |  | 3. COUNTRY  |                             |
| 4. U.S. CITIZEN? (If no, answer question 5)  |         |                             | 5. LIST IMMIGRATION DOCUMENT TITLE, DOCUMENT NUMBER, AND EXPIRATION DATE (If applicable) |   |                             |
| <b>Section III. WARNING: CONSENT TO SUBJECT SEARCH/SEIZURE, VEHICLE TOWING, REIMBURSEMENT, IMPOUNDMENT</b>   |         |                             |  |   |                             |
| By accepting this pass you give your consent to search of your vehicle while it is entering on, or leaving Fort Benning. If your vehicle is towed or impounded, you agree to reimburse the towing agent on behalf of the vehicle owner/operator.   |         |                             |  |   |                             |
| _____ <b>Initial</b>   |         |                             |  |   |                             |
| <b>Section IV: ATTESTATION</b>   |         |                             |  |   |                             |
| I attest to the fact that I have been briefed by my sponsor and understand the purpose for the NCIC check. I understand the information on this form is being collected in accordance with 50 U.S.C., Section 797, and DoD 5200.8, and federal laws. Permitting the installation commander to limit access to the installation for security reasons and that this data will be used to screen personnel who have or are seeking access Fort Benning. I have voluntarily completed this form and shall provide the Army a specimen of my fingerprints, if/when requested. I hereby give my consent and authorization for the Army to conduct any additional background screenings deemed necessary over the next 12 months, to include comparing/checking my fingerprints against local, state, and federal criminal databases. I understand (a) criminal offense(s) may be prosecuted in federal court. The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willfully false statement on this application can be punished by fine or imprisonment or both (18 U.S.C section 1001). |         |                             |  |   |                             |
| <b>I understand approvals/denials take 3-5 working days and can be verified by phone by calling the Visitor Center, M-F, 7:30am-5pm (706-544-9103/706-544-9124).</b>   |         |                             |  |   |                             |
| Applicant Signature: _____   |         |                             |  | Date: _____                                       |                             |
| Fort Benning Sponsoring Agency name (i.e. 2 CES, AAFES, Base Education Office): _____  |         |                             |  |   |                             |
| <b>ACCESS DENIALS.</b> If denied, you may appeal in writing to the Garrison Commander. If you appeal, you must provide a copy of supporting documentation (i.e. court minutes, expunged records, etc.) that may mitigate your security issues to the Visitor Center at Lindsey Parkway.  |         |                             |  |   |                             |
| <b>Section V. FOR USE BY FORT BENNING SPONSORING ORGANIZATION OR AGENT CARD/VISITOR SPONSOR ONLY</b>   |         |                             |  |   |                             |
| <b>1.) Days of the week and hours requesting authorization to enter Fort Benning. (Circle all that apply)</b>  |         |                             |  |   |                             |
| <u>  </u> <u>  </u> <u>  </u> <u>  </u> <u>  </u> <u>  </u> <u>  </u><br><b>M. Tu. W. Th. F. Sa. Su.</b>   |         |                             |  |   |                             |
| Dates of pass: _____   |         | Earliest hour: _____        |  | AM / PM   | Latest hour: _____          |
| AM / PM  |         |                             |  |   |                             |
| Fort Benning sponsoring organization/agency (i.e. 2 CES, AAFES, Base Education Office): _____  |         |                             |  |   |                             |
| <b>2.) Print contact information of Fort Benning sponsor/base agency representative:</b>   |         |                             |  |   |                             |
| Last Name: _____   |         | First Name: _____           |  | Middle Initial: _____                             |                             |
| Social Security Number [ _____ ]   |         |                             |  |   |                             |
| Title/Rank: _____  |         | Phone: _____                |  | Email: _____                                      |                             |
| _____  |         |                             | _____  |   |                             |
| <b>Signature</b>   |         |                             | <b>Date</b>  |   |                             |
| Completed form signed by Fort Benning sponsor turned in to Visitor Center at Lindsey Parkway Fort Benning Georgia  |         |                             |  |   |                             |
| <b>Section VI. PRIVACY ACT STATEMENT</b>   |         |                             |  |   |                             |
| Authority: 50 USC Section 797; E.O.9397  |         |                             |  |   |                             |
| <b>PRINCIPAL PURPOSE(S):</b> The purpose for requesting personal information is to assist Access Control personnel in documenting contractor employee suitability for access to Fort Benning. Social security number and date of birth are necessary to identify the person and records. This information may be used to determine suitability of person desiring access to Fort Benning; as well as, for lawful purposes including law enforcement and litigation. This information will be used to generate state and federal criminal history records checks.   |         |                             |  |   |                             |
| <b>INTENDED USE:</b> For all personnel who are not authorized a Common Access Card (CAC) and require regular and frequent access to the installation in performance of their official duties.  |         |                             |  |   |                             |
| <b>DISCLOSURE:</b> Disclosure of requested information is voluntary; however, failure to provide information will result in access privileges being refused or withdrawn. The Privacy Act Statement will apply throughout the duration of the Air Force contract while serving in the capacity of prime contractor or subcontractor/supplier employee.   |         |                             |  |   |                             |

| FORT BENNING GEORGIA ACCESS REQUEST FORM<br>(THIS FORM IS SUBJECT TO THE PRIVACY ACT OF 1974)  |         |                             | ATTENDANCE TO FAMILY DAY,<br>GRADUATION OTHER SPECIAL EVENT                              |                             |                   |
|--|---------|-----------------------------|--|-----------------------------|-------------------|
| Complete this form and return to your Fort Benning sponsor. A National Crime and Information Center (NCIC) check will be conducted prior to granting access to the installation. By signing this application, you affirm/swear the information provided is true. That a knowing and willful false statement on this application can be punished by barment from the installation, a fine, imprisonment or both. (18 U.S.C. Section 1001). Furthermore, that under the authority of 50 U.S.C. Section 797 and DoD 5200.8, the installation commander has imposed a continuing obligation for you to disclose to Fort Benning, within 24 hours, if you're convicted of any criminal offenses that occur while you have unescorted access authority to Fort Benning   |         |                             |  |                             |                   |
| <b>Section I. PERSONAL INFORMATION</b>   |         |                             |  |                             |                   |
| 1. NAME (Last, First, Middle)  |         | 2. DRIVER'S LICENSE #/State | 3. Social Security Number  | 4. DATE OF BIRTH (YYYYMMDD) |                   |
| 5. CURRENT ADDRESS (Include City/State/ZIP Code)   |         |                             | 6. HOME PHONE NUMBER   |                             | WORK PHONE NUMBER |
| 7. SEX   | 8. RACE |                             | 9. EYE COLOR   | 10. HAIR COLOR              | 11. HEIGHT        |
|  |         |                             |  |                             | 12. WEIGHT        |
| <b>Section II. PLACE OF BIRTH</b>  |         |                             |  |                             |                   |
| 1. CITY  |         | 2. STATE (If applicable)    |  | 3. COUNTRY                  |                   |
| 4. U.S. CITIZEN? (If no, answer question 5)  |         |                             | 5. LIST IMMIGRATION DOCUMENT TITLE, DOCUMENT NUMBER, AND EXPIRATION DATE (If applicable) |                             |                   |
| <b>Section III. WARNING: CONSENT TO SUBJECT SEARCH/SEIZURE, VEHICLE TOWING, REIMBURSEMENT, IMPOUNDMENT</b>   |         |                             |  |                             |                   |
| By accepting this pass you give your consent to search of your vehicle while it is entering on, or leaving Fort Benning. If your vehicle is towed or impounded, you agree to reimburse the towing agent on behalf of the vehicle owner/operator.   |         |                             |  |                             |                   |
|  |         |                             |  |                             | Initial           |
| <b>Section IV: ATTESTATION</b>   |         |                             |  |                             |                   |
| I attest to the fact that I have been briefed by my sponsor and understand the purpose for the NCIC check. I understand the information on this form is being collected in accordance with 50 U.S.C., Section 797, and DoD 5200.8, and federal laws. Permitting the installation commander to limit access to the installation for security reasons and that this data will be used to screen personnel who have or are seeking access Fort Benning. I have voluntarily completed this form and shall provide the Army a specimen of my fingerprints, if/when requested. I hereby give my consent and authorization for the Army to conduct any additional background screenings deemed necessary over the next 12 months, to include comparing/checking my fingerprints against local, state, and federal criminal databases. I understand (a) criminal offense(s) may be prosecuted in federal court. The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willfully false statement on this application can be punished by fine or Imprisonment or both (18 U.S.C section 1001). |         |                             |  |                             |                   |
| <b>I understand approvals/denials take 3-5 working days.</b>   |         |                             |  |                             |                   |
| Applicant Signature: _____   |         |                             | Date: _____  |                             |                   |
| Return email address : _____   |         |                             |  |                             |                   |
| <b>ACCESS DENIALS.</b> If denied, you may appeal in writing to the Garrison Commander. If you appeal, you must provide a copy of supporting documentation (i.e. court minutes, expunged records, etc.) that may mitigate your security issues to the Visitor Center at Lindsey Parkway.  |         |                             |  |                             |                   |
| <b>Section VI. PRIVACY ACT STATEMENT</b>   |         |                             |  |                             |                   |
| Authority: 50 USC Section 797; E.O.9397  |         |                             |  |                             |                   |
| <b>PRINCIPAL PURPOSE(S):</b> The purpose for requesting personal information is to assist Access Control personnel in documenting contractor employee suitability for access to Fort Benning. Social security number and date of birth are necessary to identify the person and records. This information may be used to determine suitability of person desiring access to Fort Benning; as well as, for lawful purposes including law enforcement and litigation. This information will be used to generate state and federal criminal history records checks.   |         |                             |  |                             |                   |
| <b>INTENDED USE:</b> For all personnel who are not authorized a Common Access Card (CAC) and require regular and frequent access to the installation in performance of their official duties.  |         |                             |  |                             |                   |
| <b>DISCLOSURE:</b> Disclosure of requested information is voluntary; however, failure to provide information will result in access privileges being refused or withdrawn. The Privacy Act Statement will apply throughout the duration of the Air Force contract while serving in the capacity of prime contractor or subcontractor/supplier employee.   |         |                             |  |                             |                   |



**DEPARTMENT OF THE ARMY**  
US ARMY INSTALLATION MANAGEMENT COMMAND  
ATLANTIC REGION  
GARRISON COMMAND  
1 KARKER STREET, BUILDING 4, SUITE 5900  
FORT BENNING, GEORGIA 31905-5000

Reply to  
Attention of

Office of the Commander

01 December 2014

Dear Family and Loved Ones,

Congratulations, your loved one has become a member of the finest fighting force in the world. We share in the pride of your Soldier's accomplishment and to help facilitate your ability to share in your Soldier's Graduation Ceremony, please plan your travels with the below requirements in mind.

Fort Benning Military Reservation requires identity proofing and vetting personnel not affiliated with the Department of Defense (DoD). Those who do not have a U.S. Government Common Access Card (CAC) and/or Uniformed Services Identification (ID) Card, and wish access to Fort Benning, will be checked through the National Crime Information Center Interstate Identification Index (NCIC-III) before being granted unescorted access onto the installation.

The NCIC-III check is used to determine fitness for granting unescorted access to the installation. If derogatory information is found during the check, access will be denied.

Such derogatory information includes, but is not limited to, the following:

- a. Criminal arrest information about the individual that causes the Installation Commander to determine that the individual presents a potential threat to good order, discipline, or health and safety on the installation.
- b. The installation is unable to verify the individual's claimed identity based on the reasonable belief that the individual has submitted fraudulent information concerning his or her identity in the attempt to gain access.
- c. The individual has a current arrest warrant in NCIC, regardless of the offense or violation.
- d. The individual is currently barred from entry to a Federal installation or facility.
- e. The individual has been convicted of crimes encompassing sexual assault, armed robbery, rape, child molestation, production or possession of child pornography, trafficking in humans, drug possession with intent to sell or drug distribution.
- f. The individual has a U.S. conviction for espionage, sabotage, treason.
- g. The individual is a registered sex offender.
- h. The individual has a felony conviction within the past 10 years, regardless of the offense or violation.
- i. The individual has been convicted of a felony firearms or explosives violation.

j. The individual has engaged in acts or activities designed to overthrow the U.S. Government by force.

k. The individual is identified in the Terrorist Screening database as known to be or suspected of being a terrorist or belonging to an organization with known links to terrorism or support of terrorist activity.

A non DoD member with a favorable NCIC-III check will be granted a visitor pass.

The specific requirements of the Visitor's Pass includes:

- a. Personal Identifiable Information (PII) submitted by the visitor in order to obtain the visitor's pass.
- b. Valid current picture identification (i.e. Drivers License, State Identification Card, Passport, etc).
- c. A NCIC-III favorable background check.

The process will take approximately 10 minutes, depending on the volume of customers, and access to NCIC-III at the Visitor Control Center (VCC).

Upon verification of your identity (Federal or State picture identification), a bar-coded, scannable visitor pass will be issued. This will provide you access onto the installation at any Access Control Point (ACP) during your visit.

Sincerely,

MICHAIL S. HUERTER  
COL, IN  
Garrison Commander



REPLY TO  
ATTENTION OF

**DEPARTMENT OF THE ARMY**  
US ARMY INSTALLATION MANAGEMENT COMMAND  
ATLANTIC REGION  
HEADQUARTERS, UNITED STATES ARMY GARRISON  
1 KARKER STREET, BUILDING 4, SUITE 5900  
FORT BENNING, GEORGIA 31905-4500

Policy Memorandum AFI 36-3026

IMBE-HRM-S

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Retrieval of Common Access Card (CAC) from Contractors at Expiration of Contract or Termination

1. REFERENCES:

a. DoD Instruction 5200.46, DoD Investigation and Adjudication Guidance for Issuing the Common Access Card (CAC), 9 SEP 14

b. DoD Manual 1000.13, Vol 1, DoD Identification (ID) Cards: ID Card Life-Cycle, 23 JAN 14

c. AFI 36-3026\_IP, 17 JUN 2009, Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel

d. ALARACT 285/2013, 25 OCT 13, Subject: Enhancing Protection of Army Installations, Facilities, and Workplaces

e. Secretary of the Army Memorandum, 31 OCT 2013, Subject: Uncleared Contractor Common Access Card Credentialing and Installation Access

f. Fort Benning DPTMS Policy Memorandum, Subject: Industrial Security Program, which includes Common Access Card (CAC) Credentialing and the Contract Security Classification Specification, DD Form 254 for Contractors

2. PURPOSE: To provide guidance and clarification on who is responsible for retrieving and returning CACs to the Installation ID Card Section from contractors who are no longer employed by the installation. This memorandum also provides guidance to gate guards regarding confiscation of mutilated, expired or altered CACs and Military ID cards.

3. POLICY:

a. CACs issued to contractors are required to be turned in upon completion of the contract duration or upon termination of employment by that contractor.

b. The government employee with primary responsibility to ensure completion of CAC turn-in is the Contracting Officer Representative (COR) or the Quality Assurance Representative (QA). The COR or QA shall establish procedures to ensure that the issuance and retrieval of CACs are part of the normal personnel check-in and check-out processes. These procedures will identify when CACs are to be turned in and who will have responsibility to retrieve them. After retrieval, CACs are to be turned in to the Installation ID Card Section once a week using a DA Form 200 (Transmittal Record). CORs/TAs have front of the line privileges at the ID Card Section in order to turn in CACs. Please identify yourself as performing that mission and the ID Card Section employee will get to you next. After verification of CACs received, the ID Card Section employee will sign the DA Form 200 and take possession of the CAC.

IMBE-HRM-S

SUBJECT: Retrieval of Common Access Card (CAC) from Contractors at Expiration of Contract or Termination

c. If the CAC cannot be retrieved from the contract employee, the Contractor Site Manager, or equivalent, will immediately provide a memorandum to the Installation ID Card Section, and to the appropriate Trusted Agent (TA), explaining why the CAC could not be retrieved. Upon receipt of this memorandum, the TA will immediately revoke the CAC in the system and then send the memorandum to the Military Police (MP) Station. The MP Station will enter this information into their database.

d. The TA is the government representative who ensures that only authorized individuals are issued CACs. The TA will ensure the contractor was properly vetted through his Supporting Security Manager (SSM) with a favorable FBI Fingerprint check and NACI initiated. JPAS will reflect a date in the PSQ Sent. These actions will be documented and provided to the TA. Applications for contractor CACs are processed, verified and approved by the TA using the Trusted Associate Sponsor System (TASS). TAs are required to verify contractor CAC privileges every 180 days. If the contractor is no longer employed for that contract or does not have the appropriate favorable adjudicated investigation, the TA will take immediate action to revoke the CAC in the system. This is an added measure to ensure CACs are terminated when no longer needed.

e. If the CAC is lost or destroyed, the contractor shall sign a statement to explain the conditions of loss or destruction and provide a copy to the COR or QA. The COR or QA will further provide that statement to the TA. The TA will re-verify vetting with the SSM and then process another CAC application in TASS to replace the lost or destroyed card. When application is approved, the contractor shall make an appointment with the ID Card Section and must bring a copy of the signed statement and two valid forms of identification to obtain the new CAC.

f. If the CAC is stolen, the contractor shall report this theft at the Military Police (MP) Station. The MP Station will provide documentation (FB DES Form 121 and DA Form 2823) to the contractor for use when applying for a replacement card. The contractor shall provide a copy of this documentation to the COR or QA who will follow the same process identified in paragraph 3e above. The TA will not process another CAC application in TASS without this documentation. This documentation must also accompany the contractor at appointment with the ID Card Section.

g. Gate guards at all Installation Access Points are required to confiscate all CACs/Military ID cards that are mutilated, expired or altered and provide these individuals a document of confiscation that gives instructions on how to obtain a replacement card. All cards confiscated by the guards are to be turned in to the Installation ID Card Section weekly using DA Form 200 (Transmittal Record). Please follow same process identified in paragraph 3b, above, when turning in cards at the ID Card Section.

h. Unauthorized possession of an official identification card, like a CAC, can be prosecuted criminally under section 701 of title 18, United States Code (U.S.C.), which prohibits photographing or otherwise reproducing or possessing DoD identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both.

i. Organization sponsoring contracts will work with supporting contracting offices to ensure CAC security clauses and retrieval responsibilities are incorporated in the contract performance work statement.

j. This memorandum supersedes Policy Memorandum 36-3026-1, 28 FEB 2014.

IMBE-HRM-S

SUBJECT: Retrieval of Common Access Card (CAC) from Contractors at Expiration of Contract or Termination

4. PROPONENT: DEERS/RAPIDS Office, Military Personnel Services Branch, 706-545-6812/8206.

FOR THE COMMANDER:

MICHAIL S. HUERTER  
COL, IN  
Garrison Commander

DISTRIBUTION:

ADMIN L, CSM/SGM, MSC DCO/XO, MCoE/Tenant BN CDRs Lists, Contractng Officer  
Representatives, Security Managers, Trusted Agents

IMBE-PLS

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Industrial Security Program for Common Access Card (CAC) Credentialing and Contract Security Classification Specification (DD Form 254) Development.

1. REFERENCES:

a. Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information" 30 JUN 08

b. Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," 27 AUG 04

c. DoD Instruction 5200.46, DoD Investigation and Adjudication Guidance for Issuing the Common Access Card (CAC), 9 SEP 14

d. DoD Manual 1000.13, Vol 1, DoD Identification (ID) Cards: ID Card Life-Cycle, 23 JAN 14

e. U.S. Secretary of the Army Memorandum, Subject: Uncleared Contractor Common Access Card Credentialing and Installation Access, 31 OCT 13

f. U.S. Office of Personnel Management (OPM) Memorandum, "Introduction of Credentialing, Suitability and Security Clearance Decision-Making Guide," 12 JAN 08

g. U.S. OPM Federal Investigation Notice (FIN) Number 06-04, "HSPD 12 – Advanced Fingerprint Results," 8 JUN 06

h. U.S. OPM FIN Number 15-03, "Implementation of Federal Investigative Standards for Tier 1 and Tier 2 Investigations," 4 NOV 14

i. Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System (TASS) Trusted Agent User Guide, MAR 13

j. Headquarters Department of the Army G-2 DD Form 254 Preparation Guide, FY1

k. AR 380-49, Industrial Security Program, 20 MAR 13

l. Fort Benning Directorate of Human Resources (DHR) Policy Memorandum, Subject: Retrieval of Common Access Card (CAC) from Contractors at Expiration of Contract or Termination, NOV 14

IMBE-PLS

SUBJECT: Industrial Security Program for Common Access Card (CAC) Credentialing and Contract Security Classification Specification (DD Form 254) Development.

2. PURPOSE: This memorandum establishes the Fort Benning Industrial Security Program, which includes responsibilities for 1) CAC Credentialing and 2) Contract Security Classification Specification (DD Form 254) development.

3. POLICY:

a. COMMANDER/DIRECTOR will:

(1) Establish the Industrial Security Program in their command, activities and areas of responsibilities.

(2) Ensure supporting security managers (SSM), trusted agents (TA) and contracting officer representatives (COR) abide by this policy and participate in the HSPD-12 Working Group.

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

b. SUPPORTING SECURITY MANAGER (SSM) will:

(1) Be a Federal employee with a minimum eligibility of Secret and active CAC.

(2) Comply with and implement this instruction and AR 380-49.

(3) Review Joint Personnel Adjudication System (JPAS) records for all contractors receiving CACs.

(4) Provide written documentation to the TA whether the contractor has an Interim or Final credential and can receive a CAC.

(a) Interim credentialing is authorized when JPAS records show a favorable Fingerprint record and NACI/Tier 1 or greater investigation has been submitted to the Investigative Service Provider (ISP), which is Office of Personnel Management (OPM). To clarify: The JPAS record will show a completed (open and close date) for a Special Agreement Check (SAC) and a current date in the "PSQ Sent Date". Please contact your organization's security liaison at the Directorate of Plans, Training, Mobilization and Security (DPTMS) Security Division for specific training or assistance.

(b) Final credentialing is authorized when JPAS records clearly show a favorable NACI/Tier 1 or higher determination or eligibility in the "Eligibility" and "Investigation" located under the SSN and EDI PN number.

(5) Complete and validate DD Form 2875, Part III for Fort Benning Nonsecure Internet Protocol Router Network (NIPRNet) for either the Interim or Final CAC.

IMBE-PLS

SUBJECT: Industrial Security Program for Common Access Card (CAC) Credentialing and Contract Security Classification Specification (DD Form 254) Development.

(a) Interim credential: Item 28a, Date of Investigation is JPAS PSQ Sent Date.

(b) Final credential: Item 28a, Date of Investigation is JPAS Investigation Close Date listed in the Investigation line located under the SSN and EDI PN number.

(c) Item 28b, Clearance Level: All NACI/Tier 1 Investigations are for un-cleared, non-sensitive positions; annotated as "NONE". Cleared contractors working on classified contracts annotate highest level of eligibility required for the contract.

(6) Provide in and out processing in the appropriate category in JPAS. Note: Contractors who require **only** a NACI/Tier 1 investigation must receive a generic Industry category with the Army as the component. In and out processing includes providing the IT Level.

(a) IT level 3 requires initial or final credentialing and is required for general user access to Government information systems.

(b) IT level 2 requires a minimum eligibility of and is required for Government data-bases, like JPAS or elevated privilege on workstations, systems and/or networks.

(c) IT level 1 requires a minimum eligibility of Top Secret, required for privileged access on a classified network (e.g. SIRPNet).

(7) Initiate NACI/Tier 1 when no other favorably adjudicated personnel security investigation is annotated in JPAS. Always check with your security liaison, because they have access to OPM's Central Verification System, which contains current NACI/Tier 1 investigations.

(a) Verification of U.S. Citizenship: Personnel Security Investigation Center of Excellence (PSI-CoE) requires verification of U.S. Citizenship. Passports are not a valid form of citizenship verification. Please review the PSI-CoE regulatory guidance or contact your security liaison.

(b) Initiate NACI/Tier 1 investigation and annotate the following :

- i. Reason for Access: Select HSPD-12
- ii. Security Office Identifier (SOI): DODH
- iii. Upload the OF 306, Declaration for Federal Employment (Oct 11)

(c) Send the individual to DPTMS Security Division for fingerprints: For hours of operation and directions call 706-545-3048 or 545-9736.

IMBE-PLS

SUBJECT: Industrial Security Program for Common Access Card (CAC) Credentialing and Contract Security Classification Specification (DD Form 254) Development.

(8) Report all adverse information, suspicious contacts and other reportable incidents to DPTMS Security Division on a DA Form 5248-R.

(9) Provide or ensure the contractor receives a security briefing from the organization's COR, SSM or TA. The briefing must include the following elements:

(a) The Contractor is responsible to account for and protect the CAC.

(b) The CAC shall be returned to the organization immediately upon any of the following events:

i. When no longer needed for contract performance.

ii. Upon completion of the Contractor employment.

iii. Upon contract completion or termination.

(c) The contractor is only authorized to use the CAC for the specific contract, unless they receive written authorization from the COR. For instance, the contractor cannot use the CAC to visit another military installation, unless it is authorized by the contract or COR.

(d) The contractor must report, in writing, any adverse information, suspicious contacts and other reportable incidents to the COR, TA or SSM.

b. TRUSTED AGENT (TA) will:

(1) Be a Federal employee and have a minimum of a favorable NACI/Tier 1 investigation and a current CAC.

(2) Comply with and implement this instruction, the Trusted Associated Sponsorship System (TASS) User Guide and the Fort Benning DHR Policy Memorandum, Subject: Retrieval of Common Access Card (CAC) from Contractors at Expiration of Contract or Termination.

(3) Provide SSM potential contractors' social security numbers for verification.

(4) Collaborate with SSM and **ONLY initiate TASS process when provided written confirmation** the contractor has the required favorable investigation for an interim or final credentialing required for a CAC.

(5) Prior to TASS initiation, identify contractor using two original source identification, one must be a Government photo ID, in accordance with DoDI 5200.46.

IMBE-PLS

SUBJECT: Industrial Security Program for Common Access Card (CAC) Credentialing and Contract Security Classification Specification (DD Form 254) Development.

- (6) Re-verify with SSM and COR, then reapprove each CAC every 180 days.
- (7) In accordance with TASS User Guide, maintain less than 100 active CACs.
- (8) Report any adverse information, suspicious contacts and other reportable incidents by submitting information and any documents in writing to the COR and SSM.
- (9) Maintain the following records for all active and 90 days for inactive CACs:
  - (a) Written verification from security stating contractor has interim or final credentialing to receive a CAC.
  - (b) Interim credentialing decisions must be re-verified every 30 days.
  - (c) CAC turn in records from ID Section. See the Fort Benning DHR Policy Memorandum, Subject "Retrieval of Common Access Card (CAC)" for details, especially when the CAC is not retrieved, in a timely manner.
  - (d) Derogatory reports sent to SSM or directly to DPTMS Security Division.

c. CONTRACTING OFFICER REPRESENTATIVE (COR) will:

- (1) Be a Federal employee and have a minimum of a favorable NACI/Tier 1 investigation for unclassified contracts and/or final eligibility and access at the highest level stated in the classified contract.
- (2) Comply with and implement this instruction and AR 380-49.
- (3) Provide our office with following documents and information for completion of the DD Form 254:
  - (a) Performance Work Statement
  - (b) Period of Performance
  - (c) Fillable DD 254 with items 4, 5, 6a, 6b, 8a, 8b, 8c, 9, 10, 11, 14 and any information for required comments in block 13 based on items checked in blocks 10 & 11 and complete COR contract information. Guidance for required comments can be found in the current DA G-2 DD Form 254 Preparation Guide.
  - (d) AMO number if coordinated via TRADOC Contract Database (TCD). Also include contract number if executing an option year DD254 revision.

IMBE-PLS

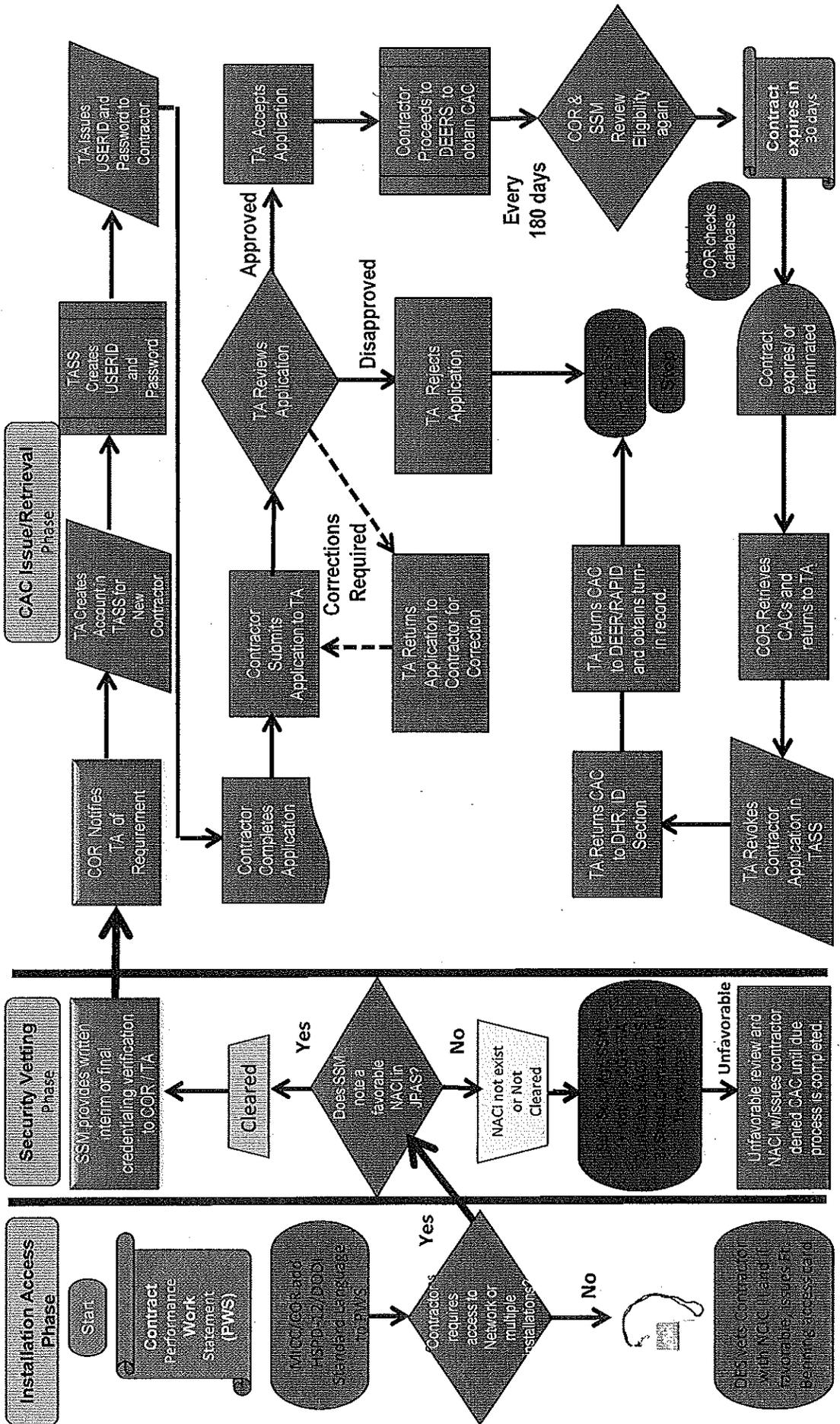
SUBJECT: Industrial Security Program for Common Access Card (CAC) Credentialing and Contract Security Classification Specification (DD Form 254) Development.

d. INSTALLATION SECURITY SPECIALIST (ISS) will:

- (1) Be a Security Specialist working with IMCOM DPTMS Security Division.
- (2) Assist and provide initial and annual HSPD-12 training to all SSM, TA and COR. Be available throughout the year for research and assistance.
- (3) Provide fingerprint processing for the Special Agreement Check (SAC). Security Assistants can also provide this administrative function.
- (4) Assist SSM with research to ensure CAC Credentialing is accomplished. Security Assistants can also provide this administrative function.
- (5) Be the lead and conduct monthly or minimum of a quarterly HSPD-12 Working Group for SSM, TA and COR. HSPD-12 WG is to maintain contact, provide current updates and ensure Industrial Security compliance.
- (6) Receive and process all credible derogatory information to the Defense Office of Appeals and Hearing (DOHA). Security Assistants can also provide this administrative function.
- (7) Receive and process all CAC Credentialing Letter of Denial or Revocation from DOHA. Security Assistants can also provide this administrative function.
- (8) Conduct annual Staff Assistance Visit to ensure the Command Industrial Security Program is maintained.

4. PROPONENT: The proponent is DPTMS Security Division, 706-545-9355.

# CAC CREDENTIALING Flowchart



DEPARTMENT OF THE ARMY  
SPECIFIC UNIT HEADER  
FORT BENNING, GEORGIA 31905-5000

XXX-XX-XX

01 December 2014

MEMORANDUM FOR Directorate of Emergency Services (ATTN: Guard Branch)

SUBJECT: National Crime Information Center Interstate Identification Index (NCIC-III)  
Checks for Unescorted Access

1. Request the roster of attached personnel be vetted through NCIC-III in accordance with the requirements of unescorted access to the installation.
2. The Contract Number associated with each employee is annotated on the attachment or Memorandum of Understanding/Agreement (IF APPLICABLE)
3. The point of contact is the undersigned at 706.XXX.XXXX or XXXXXX.XXXXX.civ@mail.mil.

STANDARD SIGNATURE BLOCK  
TITLE  
ORGANIZATION

**HSPD-12 ID Card Request**

Full Name: \_\_\_\_\_

DOB: \_\_\_\_\_

SSN: \_\_\_\_\_

Circle One: Male / Female

Other Names Used: \_\_\_\_\_

I understand that the information provided above will be utilized to conduct background screening for the purpose of obtaining a Fort Benning installation access card.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date



