Military Police

JOINT BASE MYER-HENDERSON HALL INSTALLATION ACCESS CONTROL POLICY

JBM-HH REG 190-13 ACP, Dated 21 January 2026

Distribution Restriction Statement
This regulation contains technical or

operational information that is for official Government use only. Distribution is limited to US Government agencies.

Destruction Notice.

AUTHORITY:

SANDOVAL.KEITH.PAUL.1179106112

Digitally signed by SANDOVAL.KEITH.PAUL.1179106112
Date: 2026.01.30 10:23:52 -05'00'

KEITH P. SANDOVAL
COL, AV
Commanding

Joint Base Myer-Henderson Hall (JBM-HH) Installation Access Control

Summary. This regulation prescribes policies and procedures for granting access to Fort Myer-Henderson Hall.

Applicability. This regulation applies to Department of Defense (DoD) employees, contractors and all units, organizations or activities assigned, attached or tenant to Joint Base Myer - Henderson Hall (JBM- HH) JBM-HH. This regulation does not authorize methods of operation or requirements outlined or specified by higher command to be changed in any manner. In the case where this regulation may conflict with a higher command's requirement or regulation, the more stringent standard of the two will apply. Questions concerning the applicability and interpretation of contents should be referred to the Directorate of Emergency Services (DES) (ATTN: Physical Security Office).

Proponent. The proponent for this regulation is the Physical Security Office, DES Fort Myer, VA 22211.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval of the Installation Physical Security Office, DES. Commanders (CDRs)/Directors (Dir)/ Facility Managers (FMs) will not deviate from or supplement this regulation.

Suggested Improvements. Users are invited to send comments and suggested improvements on Department of Army (DA) Form 2028, Recommended Changes to Publications and Blank Forms, directly to Director, DES (ATTN: Physical Security Office, (AMIM-MHL).

Distribution. This publication is available in electronic media only and is limited for official Government use only.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction
Purpose ● 1-1, page 3
References ● 1-2, page 3
Administrative Control ● 1-3, page 3

Chapter 2
General
Scope ● 2-2, page 3
Authority ● 2-2, page 3
Policy● 2-2, page 3

Chapter 3
Access Control Procedures
Authorized Personnel ● 3-1, page 4
Screening for Unauthorized Personnel ● 3-2, page 6
Vetting ● 3-3, page 7
Fitness Determinations ● 3-4, page 8
Credentialing ● 3-5, page 9
Sponsorship ● 3-6, page 11
Foreign National Visitors ● 3-7, page 12
Special Events ● 3-8, page 13
Rideshare ● 3-9, page 15
Trusted Traveler Program (TTP) ● 3-10, page 18
Debarment ● 3-11, page 19

Chapter 4
Commercial Vehicles
Commercial and Delivery Vehicles ● 4-1, page 20
Moving Companies ● 4-2, page 20
Tow Trucks ● 4-3, page 20
Taxi Companies, Transportation Buses ● 4-4, page 21
Food Delivery Vehicles and Vendors ● 4-5, page 22

Chapter 5
ACP Active Vehicle Barrier (AVB) Activation Procedures
Roles and responsibilities ● 5-1, page 22
Procedures ● 5-2, page 22
Training ● 5-3, page 24
Safety Considerations ● 5-4, page 24
Punitive Action ● 5-5, page 24

Chapter 6
Limited Use Gates
Page 25

Appendixes

A. References
B. Acronym Definitions
C. Joint Base Myer – Henderson Hall Installation Access Request Form 190-16X
D. JBM-HH Access Denial Waiver Packet
E. JBM-HH Installation Support Request Form-7
F. Fitness Determination Evaluation Guide

Chapter 1
Introduction

1-1. Purpose
To establish policy and standardize access control requirements for personnel entering Joint Base Myer-Henderson Hall (JBM-HH), Fort Myer, Virginia, Henderson Hall, Virginia and Fort McNair, District of Columbia. This police describes the requirements for vehicle and personnel screening, vetting, identification documents, passes and general access control procedures.

1-2. References
Required and related publications are listed in appendix A.

1-3. Administrative Control
The Directorate of Emergency Services (DES) is responsible for the management and control of installation access.

Chapter 2
General

2-1. Scope
To standardize access control requirements for entering JBM-HH relating to vehicle and personnel screening, identification (ID) documents, vehicle registration, long term access control Automated Installation Entry (AIE) tokens, card, and temporary passes in accordance with (IAW) AR 190- 13, chapter 8. Nothing in this policy is intended to limit the Commander's authority to further limit access based upon, but not limited to, local security requirements, increased Force Protection Condition (FPCON) levels and emergencies.

2-2. Authority
Authority to control access to United States Army (USA) installations varies based on jurisdiction, property rights, and geographic location. Within United States (US) jurisdiction, commanders (CDRs) publish and enforce guidance to protect installation resources IAW Department of Defense (DoD) and USA policy. In addition, DoD Instruction (DoDI) 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), prohibit individuals from entering military installations within the jurisdiction of the US for a purpose prohibited by law or lawful regulation, or reentering an installation after being ordered not to reenter by any officer in command of the installation.

2-3. Policy
IAW Army Regulation 190-13, Army Directive 2014-05 and Headquarters Department of the Army EXORD 033-15, all personnel desiring escorted or unescorted access to Army installations will enter the installation through authorized Access Control Points (ACP) and must be vetted using the National Crime Information Center (NCIC) Interstate Identification Index (III) and The Terrorist Screening Database (TSDB). Security personnel will verify the Identification of all persons entering JBM-HH through the installation's Visitor Control Centers (VCC) and Access Control Points (ACPs) IAW

appendix A. The Senior Commander (SC), Joint Base Commander (JBC), or delegate is authorized to grant case-specific exceptions to any and all procedures contained herein.

Chapter 3
Access Control Procedures

3-1. Authorized Personnel

a. Persons in possession of the following IDs are authorized unescorted access onto JBM-HH. Unescorted persons requesting access onto JBM-HH must have a valid purpose and an authorized form of ID. Unescorted access to JBM-HH is normally reserved for the below listed categories, unless Random Antiterrorism Measures (RAM) or an increase of Force Protection Conditions (FPCONs) are directed:

b. DoD Common Access Card (CAC): Per DoDI 8190.3, the DoD CAC is the standard ID card for Active and Reserve uniformed personnel, DoD Civilian employees, eligible contractors and some designated foreign nationals. The DoD CAC shall be the principal access control card which enables access to buildings, facilities, installations, and some limited controlled spaces.

c. Department of Defense (DD) Form 2 and DD 1173. The Uniformed Services ID and Privileges Card, (DD Form 2 and DD Form 1173) and the Armed Force of the United States Geneva Conventions Identification Card that are issued to military dependents and retirees in the manually prepared paper card form or machine-readable Teslin card format.

d. Automated Installation Entry (AIE) Token, Pass or Card. The pass or card provides a means to effectively screen a population that does not necessarily have DoD affiliation (i.e., visitors, contractors, sub-contractors, vendors, etc). The pass/card is an access credential issued by JBM-HH VCCs to persons who successfully pass a National Crime Information Center – Interstate Identification Index (NCIC-III) and Terrorist Screening Data Base (TSDB) background check and who do not otherwise meet the requirements for a CAC.

e. Other acceptable forms of ID include:

1. DD Form 2765, Veterans Health Identification Card (VHIC), and DoD Civilian Retiree Identification Card.

2. Air Force (AF) Form 354, Civilian ID card.

3. DD Form 489, Geneva Convention ID card for Civilians.

4. DA Form 1602, Civilian ID card.

5. DD Form 1934, Geneva Convention ID card for Medical and Religious Personnel.

6. DD Form 2765: Department of Defense/Uniformed Services Identification and Privilege card.

7. DD Form 2764: US DoD/Uniformed Services Civilian Geneva Convention ID.

8. Blue striped CAC (for non-U.S. citizens). Since July 2015, all CACs have been issued with an affiliation color code in a white circle under the expiration date, including “W” for white, “G” for green, and “B” for blue. These changes are meant to make it easier for visually color-impaired security officials to identify bearers who are military, Government, contractor civilians, or foreign nationals. The new format will only be issued for new and expiring cards. The blue striped CAC (for non-U.S. citizens) is a valid DOD ID credential and may be used for unescorted installation access. These CACs state “Identification Card” on the bottom front of the card. Blue striped CACs must be registered in AIE to associate the person with the local installation. Installations without AIE will perform a visual check of the card and picture to authenticate before allowing access. Dependents of blue striped CAC holders can receive an installation pass. Newly hired foreign national personnel will be issued an AIE local pass (up to 6 months) while they wait for their CAC application to be approved. When the new hire person receives their blue-striped CAC, replace their installation pass by registering their blue-stripe CAC in AIE. The foreign identification number is the number the Defense Enrollment Eligibility Reporting System (DEERS) generates and assigns to non-U.S. citizens in conjunction with issuing a blue striped CAC or Teslin card (such as, dependent wife, DD Form 1173). If anyone with a blue striped CAC has an issue with their computer certificate or other computer or CAC related issue, they need to go to the ID card office that issues CACs.

f. Non-CAC holder contractors and vendors: May be issued local access ID with a government sponsor.

1. Contractors and vendors requiring physical access to a single Army installation or facility, but who do not require access to a DOD computer network, will have a Government-employee sponsor to provide the contractual agreement with a cover memorandum signed by a verifying officer vouching for the need for long-term access to the installation. The expiration date of the issued card will be the end date of the contract or visit, or the expiration date of the sponsor’s access control card, whichever occurs first. Sponsors will be held responsible for notifying the DES (or appropriate local installation access issuing office) of terminated contract employees and for turning in of expired or revoked ID.

2. Contractors will be processed through the Contractor Verification System for issuance of a CAC, if physical access to multiple Army installations and/or access to a DOD computer network is required.

3. Non-CAC-eligible contractors will be issued local access ID that will only be used for physical access onto the single installation or facility where it is issued. Commanders and directors will use a locally produced, temporary issue, local access ID system pass with expiration date, or a pass issued by AIE or the DBIDS, if available.

g. Other personnel requesting long-term recurring installation access:

1 Family care providers. Unit commanders and directors will use the Family care plan per AR 600–20 to review and validate requests by Soldiers for installation access for Family care providers after completion of initial identity proofing and vetting.

2. Army volunteers. The director of the activity will review and validate requests to grant unescorted installation access for Army volunteers and forward the request to the senior law enforcement official after completion of initial identity proofing and vetting.

3. Gold star and next of kin survivor Family member unescorted access. The “survivor access card” will be used for both gold star Family members and next of kin survivors. The Army’s AIE system will issue an AIE card marked “Survivor.” Installations where AIE is not yet fielded will continue to issue the DA Form 1602 (Civilian Identification Card) with “Survivor” typed in the status block

4. The next of kin Family member is a survivor of a Service member who lost their life while serving on active duty. This includes service members who lose their lives while assigned to a reserve or National Guard unit in drill status. Eligible survivors are the remarried widow or widower (widows and widowers are eligible to retain their dependent ID card), parent, child, stepchild, child through adoption, brother, half-brother, sister, and half-sister of the deceased Service member.

h. Other Federal agency personnel with an approved ID document.

1. Federal, state, and local government officials driving official or emergency vehicles (non-emergency capacity) or privately owned vehicles (POVs) must present their credentials (photo ID and DL). Any Federal, state, local law enforcement, Federal Bureau of Investigation (FBI) Washington Field Office Joint Operations Center (WFO JOC), or United States Secret Service (USSS) affiliated personnel, who are on-duty or off-duty, but have official business and present valid official law enforcement or associated agency provided credentials with a photo ID/DL, may be granted access to JBM-HH without inspection, excepting RAM, FPCON measures. Military Police (MP), Department of the Army Civilian Police (DACP) or members of the Security Forces with questions shall contact the desk sergeant for clarifications. All federal, state, or local emergency vehicles responding to an emergency (Mutual Aid Plan) on the installation must notify the Installation police station. If advance notification has not been received, the police desk must verify the response with the appropriate emergency agency prior to access. Government (federal, state, and local) vehicles with approved dispatch/registration documents. Drivers must possess authorized photo ID documents.

i. JBM-HH will not accept security badges or locally produced identification cards as an identification document. In the National Capital Region (NCR) there are dozens of agency security badges and identification cards. Security badges or locally produced agency identification cards are designed for an individual to gain access to a specific building or area, not the JBM-HH installation. With the exception of a photograph and the person’s name, these badges/cards lack sufficient data to identify the bearer. Security badges and locally produced identification cards are not linked to a centrally accessible database which can be cross

referenced and verified by law enforcement, nor are they in compliance with Homeland Security Presidential Directive-12 (HSPD-12).

3-2. Screening for Unauthorized Personnel

a. Security Assistant personnel performing installation access control at the Visitor Control Center (VCC) will verify a person's need to have access to the installation and perform a visual inspection on all identification documents provided by visitors.

b. Unauthorized Personnel. Non-DoD affiliated persons must present one of the following forms of ID to request access to JBM-HH and are subject to screen procedures:

1. REAL ID: Visitors will need to ensure their State Identification/Driver's License is "REAL ID" compliant/Enhanced ID or have a secondary form of Identification to validate their non-compliant REAL ID regardless of online pass approval before entry is granted. Most states use "Not For Federal Purpose" language on their identifications to display if the ID is not REAL ID compliant. REAL ID compliant identifications will have a small star located on the ID. For more information on obtaining REAL ID compliant identification contact your State Department of Motor Vehicles.

2. Non-REAL ID Valid state Driver's License (DL) or state photo ID card. If the DL or ID card lacks a photo, the ID must be cross referenced with another form of acceptable photo identification.

3. Valid ID from US Territories: (e.g., Puerto Rico, Guam, Virgin Islands).

4. Valid passport from other countries that are cleared by the State Department which meet the requirements of Army Regulation (AR) 190-13, Chapter 8.

5. State Department driver's license or identification card with photo.

c. Persons that can not provide the above mentioned identification or that do not have a reason to visit JBM-HH will be turned around at the ACP or the VCC.

3-3. Vetting

b. Escorted Personnel. Escorts are required to remain with the Non- DoD person for the duration of the visit. Escorts must be in possession of an authorized DoD ID card to escort. Contractors in possession of a Common Access Card are not authorized to escort personnel that have not been formally vetted. Personnel that have undergone a NCIC-III check which is unfavorable may submit a request to be escorted on the installation with the approval of the Installation Physical Security Office. (2) Juveniles (17 and under): Do not undergo NCIC-III screening but require approved sponsorship if not a DoD ID card holder.

b. Personnel 17 years of age and under may not be screened for installation access utilizing NCIC-III. Juveniles must have approved sponsorship if they are not a DoD ID card holder. Juveniles who are driving a Privately Owned Vehicle must present either a DoD ID Card, or a valid state driver's license and must have an AIE token or pass.

c. The application packet for a JBM-HH Installation access pass (DES Form 190-16X), Request for a Joint Base Myer-Henderson Hall Installation Access Control Pass, is contained in appendix C.

1. Personnel record screening is a voluntary procedure. Personnel who do not wish to undergo screening checks will not be authorized installation access whether escorted or unescorted.

2. Personnel who are screened for JBM-HH access must sign a records release form, DES Form 190-16X, prior to record retrieval.

3. Applicants may send DES Form 190-16X, in advance of their intended entry date to https://pass.aie.army.mil/steps/terms_of_use for processing.

4. A NCIC-III and TSDB screening for non-DoD personnel attending the installation event will be waived where screening is impractical.

d. Personnel who are denied JBM-HH access may obtain a copy of the record information utilized to determine access authorization through the Virginia State Police (VSP) or state jurisdictional authority. VCC and Security personnel are unauthorized by law to disseminate record information to applicants or sponsors under any circumstances.

(1) Personnel may contact VSP at (804)-674-2131 or e-mail questions to background_checks@vsp.virginia.gov. Further information on requesting a copy of the Criminal History Records Check utilized for vetting access to JBM-HH may be obtained at http://www.vsp.state.va.us/CJIS_Criminal_Record_Check.shtm in conjunction with the form SP-167, pursuant to §19.2-389 of the Code of Virginia.

(2) Personnel who wish to request a waiver of the Criminal History access determination for JBM-HH must meet the requirements in appendix F and submit the Joint Base Myer-Henderson Hall Access Control Waiver Application.

3-4. Fitness Determinations

a. Access will be denied unless the Emergency Communication Center (ECC) has contacted the jurisdiction issuing the warrant and verified the warrant is no longer valid. (Note: The report that there is no warrant in NCIC is not sufficient).

b. If the warrant is valid with extradition, the applicant will be detained until such time as the requesting agency and JBM-HH can arrange transportation for the wanted person(s).

c. If the ECC is unable to verify that the warrant has been cleared, then the subject is to be informed of the following: “Our records show an outstanding warrant from (enter appropriate jurisdiction e.g.: Fairfax, Prince William, etc.) and you will be denied access until the warrant has been cleared.” VCC personnel will NOT relay the source of the information to the visitor

(e.g. visitors will not be told the information comes from the Bars and Suspension List or from NCIC screening) or what offense(s) the warrant(s) were issued for. Subjects are not authorized to view the information under any circumstances.

d. Personnel with unverifiable warrants will be told to contact the appropriate jurisdiction's court or law enforcement division for further information.

e. If a valid and verified warrant is returned with "no extradition requested" the applicant will be denied entry and given a waiver packet.

f. Access Determinations. The purpose of security screening is to ID those persons who may pose a threat to good order and discipline on JBM-HH by either denying them access. Unescorted access, escorted access or placing restrictions on their movement may be utilized if an access waiver is approved. The following criteria, while not all encompassing, will be used as a general guideline for determining denial of access to JBM-HH:

1. Any felony convictions within the last 10 years, regardless of the offense or violation.

2. Any record of a felony conviction for firearms or explosives violations.

3. The individual has a current arrest warrant in NCIC, regardless of the offense or violation.

4. The individual has a U.S. conviction for espionage, sabotage, treason, terrorism or murder.

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

6. The individual is identified in the 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.

7. The installation is unable to verify the individual's identity based on the reasonable belief that the individual has submitted fraudulent information concerning his or her identity in the attempt to gain access.

8. The individual is currently barred from entry or access to a Federal installation or facility.

9. 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.

10. The individual is a registered sex offender.

11. The NCIC-III contains criminal information about the individual that causes the senior commander, or their representative, to determine that the individual presents a potential threat to the good order, discipline, or health and safety on the installation. Fitness determination will be based on criteria listed in Appendix I, Fitness Determination Evaluation Guide.

12. VCC personnel will NOT relay the source of the information to the visitor (e.g. visitors will not be told that the information comes from the Bars and Suspension List or from NCIC-III screening). Subjects are not authorized to view the information under any circumstances.

a. VCC personnel will provide a waiver packet, appendix F, to any person(s) denied post access.

b. The JBC, or their designated representative, is the final approval authority for any adjudication on waiver requests for access denial.

3-5. Credentialing

a. Individuals shall be issued a separate ID card for each population category for which they qualify. In instances where an individual has been issued more than one ID card (e.g., an individual that is eligible for an ID card as both a Reservist and as a DoD contractor employee), only the ID card that most accurately depicts the capacity in which the individual is affiliated with the DoD should be utilized at any given time.

b. The visitor's state Driver's License (DL) or Real ID Compliant Identification will be used for identity proofing credential. Visitors will be granted access based on a legitimate need not to exceed one year.

c. Valid Passport issued from any government agency, valid Permanent Resident Card or valid United States work Visa provided they are escorted by an ID card holder and processed through the installation VCC office.

d. Certain categories of personnel may require badge/pass in addition to their ID. The VCC will issue a pass from an Army approved badge/ pass system, such as the AIE Token, card or pass which will contain the individual's personal data, sponsoring agency or individual, whether they have escorted or unescorted access, and an expiration date. Tokens, card and passes will be issued based on a legitimate need and will not exceed one year. AIE card will be requested through the Installation Physical Security Office, by submitting a Memorandum for Request with all required information signed by the government Sponsor. JBM-HH residents not in possession of a DoD credential may be approved for an AIE card pass by presenting their lease at the Visitor Center. Plastic passes will only be issued for up to a year not to exceed the expiration date of the lease.

e. Visitor Passes.

1. For one day access requests for events, or general access you may complete an online request through JBM-HH online website: https://pass.aie.army.mil/jbmhh. All requests should be submitted with as much advance notice as possible to ensure adequate processing and vetting time. Processing times will vary pending the number of requests in the queue. If practicable, requests should be submitted a minimum of four business days in advance of intended entry. Requests submitted less than four business days should be submitted as a short notice request; however, requests annotated as a short notice request do not guarantee processing in time for requested installation access.

2. Persons operating a motor vehicle who apply for an AIE token, card or visitor pass must submit a DES Form 190-16X with authorized DoD sponsorship; produce a valid permanent or temporary state/US Territories, valid DL, state registration and proof of insurance for the vehicle they are operating as well as any other dentification/documentation required for the category of pass requested.

3. All persons applying for an AIE token, card or visitor pass must produce a valid permanent or temporary state/US Territories ID and DES Form 190-16X with authorized DoD sponsorship.

4. The Installation VCC will issue an AIE token, card or visitor pass upon meeting all installation access requirements and successful completion of NCIC-III and TSDB background vetting IAW, paragraph 3-1c.

5. Passes are valid until midnight of the printed pass-through date.

6. Access control guards and/or security personnel will examine and scan all AIE passes during gate operations to ensure the AIE system verifies and validates the pass.

a. AIE cards and visitor passes are property of JBM-HH. All personnel who are issued AIE cards and visitor passes are subject to the following rules upon issuance.

b. Personnel acknowledge that their access may be revoked at any time without reason or notice.

c. Personnel acknowledge they must properly care for their pass or card to prevent damage or unnecessary wear.

d. Personnel acknowledge that it is prohibited to allow someone to tailgate (following someone in/out of gates without using a card/pass) or allow someone else to utilize their card or pass.

e. Personnel understand they must turn in their card/pass to the installation VCC when it has expired, further use is no longer required, the pass/card is requested by the pass sponsor, installation commander or their designated representatives and/or security forces.

f. Personnel understand they must notify their sponsor and the military police immediately to report any lost, damaged or stolen card or passes.

g. Personnel understand that their pass or card must be controlled at all times. If personnel know where their pass/card is, it is considered accounted for. If a pass or card is lost, unrecoverable or can't be accounted for, they must notify their sponsor and the military police immediately.

h. Once an AIE token, card or pass has been granted, personnel must utilize AIE equipped ACPs for unimpeded installation access with the exception of Commercial Delivery vehicles. AIE tokens, cards or passes do not negate or remove the requirement for RAM, any installation access restrictions IAW FPCON or additional security requirements imposed by the installation command.

3-6. Sponsorship

a. Only affiliated DoD ID card holders will be able to sponsor. Contractors in possession of a Common Access Card are not authorized to sponsor personnel. Sponsors are not required to remain with the Non-DoD person for the duration of the visit. All sponsors are responsible for the conduct of their guests and will inform the VCC when the sponsored individual's need for access is no longer required.

b. Personnel requesting access to the installation who require a sponsor will be vetted and approved for access as needed after completing and submitting DES Form 190-16 Version 2 to the VCC.

c. Guest/Partners of JBM-HH. The Senior Commander (SC) or their designated representative can approve Guest/Partners of JBM-HH access cards for person(s) who require recurring access to JBM-HH for functions or official business. Access cards will be issued based on the applicant's installation access requirements and vetting requirements, command sponsorship and may be issued for a maximum of one year.

1. Guest/Partner access cards are generally reserved for community or municipal leaders requiring recurring official access to installation leadership personnel (i.e., government officials, mayors, council members, school superintendents, board presidents,

community connectors, privatized military and business alliances, and city and county community partners).

2. The Garrison Commander may designate certain local, State, and Government Officials as VIPs. Once the designation is made staff will coordinate with VCC and process the VIP IAW the provisions of this program and issue an annual pass/badge or enroll that person in AIE for access.

d. Access for Lost stolen or missing Identification. Those individuals claiming to be Service Members, Authorized dependents, or DA Civilians who arrive at the ACP and claim they are assigned to JBM-HH, yet have no authorized ID in their possession, will be put in contact with their unit/ supervisor/ sponsor or the Police Desk so that an escort may be made available for access. Those individuals that have a valid Driver's License, but no military ID will provide it at the VCC to be vetted and then allowed access to the installation without an escort with a positive adjudication of the NCIC-III check. Those with valid DOD credentials not in their possession who fail vetting will be required to be sponsored by someone in possession of valid DOD credentials.

3-7. Foreign National Visitors

a. This policy addresses non-government-to-government visits and is not intended to cover all requirements for official visitors as identified in AR 380-10. Garrison, tenant and mission partner organizations that host official foreign government representatives must follow procedures in accordance with AR 380-10, appendix I, Department of the Army International Visits Program. All visits that involve the exchange of classified or other official government information must be coordinated through Foreign Disclosure channels. The DPTMS Garrison Security Office is the point of contact for these types of visits and can be reached at (703) 696-6151.

1. The Foreign Visit System-Confirmation Module will be used, by authorized persons, to confirm that a proposed official visit to JBM-HH by a Foreign Government representative has been approved through the foreign visits system, and to record the arrival of such visitors.

2. DPTMS will notify DES when official foreign visitors are scheduled to access the installation to ensure proper advisement to the ACPs. If notification has not been received the security forces or VCC personnel will contact the desk sergeant for guidance.

3. IAW AR 190-13, paragraph 8-5.d., official foreign visitors will be escorted.

b. Foreign national visitors, not on military orders or official visits, must apply for a visitor pass at the VCC. The VCC will collect full data on foreign national visitors who are not on military orders. Copies of the passport and the accompanying I-94 or I- 94W, or 1-551 for Permanent Resident Aliens, military ID, orders, and any other pertinent documentation presented will be photocopied and attached to the pass request when processing at the VCC.

c. Military personnel of foreign governments on orders for duty in the United States, who have not been issued a CAC yet are required to present their military ID card, their orders and a JBM-HH Form 190-16x to the VCC registrar for a temporary pass for 60 days, or they may submit an approved JBM-HH Form 190-16x for an AIE card for the length of their assignment, NTE one year. A photocopy of the orders and military ID will be attached to the application. If a CAC is issued after the issuance of an AIE pass; the AIE pass must be surrendered back to the JBM-HH VCC office.

d. Foreign Visitors 10 years of age or older are required to be sponsored for access to the installation. Escort must have authorized ID. Foreign Nationals will be required to be sponsored prior to entry and will be granted escorted or unescorted access as determined by the Physical Security Office / VCC.

e. Foreign Nationals that do not meet the vetting criteria will be turned around at the ACP or VCC and an Installation Management Command (IMCOM) Breach Reporting Form will be filled out.

3-8. Special Events

a. The DoD requires all installations to conduct a vetting process to determine fitness and eligibility for access. The two categories of Special Events for DoD CAC holders and non-DoD ID cardholders are Installation and Hosted events.

1. Installation events are large functions (i.e., 4th of July, air shows, Twilight Tattoo, etc.) where persons without authorized DoD credentials will be directed to specific gate(s) and security measures will be directed and/or conducted prior to entrance onto the installation and/or while on the installation.

a. The SC or GC will determine which events are Installation Events.

b. A NCIC-III and TSDB screening for non-DoD personnel attending the installation event will be waived where screening is impractical.

c. All non-DoD personnel 18 years and above are required to present a valid state photo or other authorized ID for these events.

d. All motor vehicle operators are required to present a valid DL, registration, and proof of insurance.

e. Vehicles are subject to a 100% inspection before being allowed access to the installation.

(2) Hosted events are small functions on the installation (i.e., weddings, proms, promotion ceremonies, retirements, Family reunions, birthdays, personal or residential gatherings, etc.) where DoD sponsors have the option to submit a special event access request for persons who will be in attendance and who do not possess DoD credentials. Such

persons will be directed to specific gate(s) where security measures will be directed and/or conducted prior to entrance onto the installation and/or while on the installation.

b. To host a non-military group from off base, the DoD sponsor must contact DPTMS at 703-696-3190 for a Joint Base Myer-Henderson Hall Installation Support Request Form, JBM-HH Form 7, version 4., Dated August 5, 2014. See appendix E. After the approval is received, the host/sponsor may hand deliver to the VCC or e-mail the VCC at usarmy.jbmhh.asa.mbx.des-vcc-passrequest@mail.mil from a .mil or authorized government email account, the guest list with all required information. Incomplete guest lists or lists without all information present will result in delays or denials. The request must be made 14 duty days in advance, but no later than 10 duty days prior to the event.

c. The request must contain, at a minimum, the following information: Description of event, time/duration of event, location of event, approximate number of non-DoD attendees and the sponsor/host organization, military sponsorship, total number of attendees (to include DoD ID card holders), Point of Contact (POC), E-mail, contact number and the date of request.

d. No less than 10 days prior to the event, the host / sponsor must submit completed 190-16x forms for all guests to the JBM-HH Visitor Control center at usarmy.jbmhh.asa.mbx.visitor-control.center@mail.mil for proper vetting of all personnel. If the forms are not submitted prior to the 10-day minimum advance deadline there is no guarantee that those forms can be processed.

e. The guest event access list must contain the following information for each guest over 18 years of age not possessing a valid DoD access credential:

1. Official Name: (Last, First, M.I.) – Indicate if there's no middle initial if there is not a given middle name as a matter of official record. If a suffix (Jr., III., etc.) is a part of the official name of record, please include the suffix after the middle initial.

2. Grade/Rank/Status (example; civilian (CIV), Staff Sergeant (SSG)).

3. Date of Birth.

4. Gender (male/female)

5. Sponsor's Organization/Agency.

6. Organization Phone Number.

7. Relationship to Sponsor.

f. Ensure all guests have valid form of ID (i.e. DL or state ID) to present at the ACP.

g. The approved event list will be provided to the DPTMS authorized/selected ACP for a specified period of time for the verification of guests on the day of the event. Guests arriving outside the specified period of time will proceed to the VCC for normal access, pass, issuance and screening.

h. A 100% vehicle inspection will be conducted at designated ACPs unless otherwise directed by DPTMS.

i. Upon the completion of the event all special event guests are required to depart the installation in a timely manner.

j. Special Event requests are subject to denial or cancelation based on the Commander's authority to further limit access based upon, but not limited to, local security requirements, increased FPCON levels and emergencies.

3-9. Rideshare

a. This program has been provided to military members, retirees, dependents, DoD contractors with or without Common Access Cards (CACs), non-DoD civilians, and any person(s) providing or using rideshare services who work, reside, or have a valid purpose on the Fort Myer or Fort McNair campuses of JBM-HH.

b. Rideshare providers will access the installation with their issued AIE pass and will be processed in same manner as a “contracted delivery driver.” Due to conducting business on the installation as a “contractor,” access is only granted through the Hatfield Gate for proper security screening and inspection of the vehicle prior to permitting its operator access to the installation. For the Fort McNair campus, drivers must enter through the 2nd Street SW gate.

c. Access is only for the explicit purpose of picking up or dropping off a fare or delivery of items. Providers will exit the installation immediately after contracted services are completed. There will be no staging, parking, or standing before or after services are rendered. Access for any other purpose is strictly prohibited. Violation of this policy may be cause for revocation of the rideshare provider’s access to the installation.

d. The Joint Base Commander’s office is the sponsoring organization for rideshare providers, except where an individual who meets DoD sponsorship criteria chooses to sponsor a rideshare provider. Rideshare providers who meet all eligibility criteria will be issued a rideshare-identified Automated Installation Entry (AIE) pass for a period of six months or for the duration of need, whichever is the lesser of the two periods.

1. Rideshare providers are considered contractors for the purpose of this policy, IAW Reference 1b, and will be processed accordingly.

2. The JBM-HH Trusted Traveler Program (TTP) will not be used in conjunction with the rideshare program.

e. Installation access procedures for Rideshare Providers:

1. All rideshare providers must have a valid state driver's license certified as REAL ID-compliant. Drivers must have proof of insurance and proper registration in accordance with state law in which the vehicle is registered.

2. Rideshare providers will access the installation with their issued AIE pass and will be processed in same manner as a "contracted delivery driver." Due to conducting business on the installation as a "contractor," access is only granted through the Hatfield Gate for proper security screening and inspection of the vehicle prior to permitting its operator access to the installation. For the Fort McNair campus, drivers must enter through the 2nd Street SW gate.

3. Access is only for the explicit purpose of picking up or dropping off a fare or delivery of items. Providers will exit the installation immediately after contracted services are completed. There will be no staging, parking, or standing before or after services are rendered. Access for any other purpose is strictly prohibited. Violation of this policy may be cause for revocation of the rideshare provider's access to the installation.

4. Ridesharing services will be suspended under HPCON, FPCON "D"/"Delta" or as directed by the Joint Base Commander or their designee.

5. Rideshare providers who violate these requirements, other DoD policies, regulations, state, or federal law are subject to have their installation access privileges suspended or terminated.

6. If operating a rental vehicle, rideshare providers will ensure that the rental vehicle has been paired to their business's driver profile.

7. Rideshare providers and/or their parent company are considered independent or third-party contractors and are not U.S. government-endorsed entities. Any civil complaints or grievances by providers or customers will be addressed through the appropriate companies' customer service. JBM-HH is not responsible for civil complaints or grievances between provider(s) and customer(s).

8. All criminal offenses that occur on the installation should be reported to the Directorate of Emergency Services (DES) Police for proper response. Criminal offenses that occur off the installation should be reported to the jurisdiction where the criminal offense was committed. All information collected is subject to be shared with local law enforcement for investigation purposes.

9. Arlington National Cemetery (ANC) is a separate entity not covered under this policy.

10. All costs or charges are between the provider and customer. JBM-HH or its agents are not liable or responsible for any charges or lost time due to access control procedures, time in lane, vetting, and/or vehicle inspection.

f. Rideshare providers NOT possessing DoD identification will:

1. Rideshare providers will visit the JBM-HH Hatfield Gate Visitor Control Center(VCC), 101 Carpenter Road, Fort Myer, VA 22211 Monday-Friday between the hours of from 0600-1700 hours and Saturday from 1000-1500 hours for initial vetting and pass-processing. Subsequent renewals may be extended at either VCC location.

2. Providers requesting to access JBM-HH for these services must meet established vetting requirements prior to having access to the installation for the stated purpose of conducting rideshare business.

3. Rideshare providers must be able to furnish physical documentation of proof of employment or their contractor status. This can be by an employment identification card, business license, TNC Certificate of Fitness, memorandum on company letterhead, or correspondence that identifies the individual as an employee or contractor of the affiliated provider. If a HACK license is required by the jurisdiction of operation or licensure, then the HACK license, or equivalent, must be furnished as part of the application process. TNCs in the District of Columbia, Maryland, and Virginia are regulated by each respective jurisdiction's authority.

4. Rideshare providers will be required to complete the JBM-HH Form 190-16x, Installation Access Request Form. Only U.S. Citizens may participate in this program. By signing, the applicant agrees to background checks as required by AR 190-13 against authoritative databases. Failure to agree to the required background checks will eliminate the provider from participating in the rideshare program.

g. DoD identification cards are not an authorized credential for rideshare provider access when performing rideshare services on the installation. Rideshare providers in this category will have to meet the same standards as non-DoD ID card holders and process through the policy's vetting requirements. This restriction applies to military members, family members, retirees, DoD civilians or contractors, and individuals authorized JBM-HH access for purposes other than the rideshare program.

1. Applicants must follow their individual department/agency guidance for off-duty employment. This policy does not grant permission for any outside employment.

h. RIDESHARE REQUIREMENTS FOR VERIFYING ACCESS ON JBM-HH**.** After successfully completing vetting requirements and receiving a Rideshare credential, providers are required to have a valid business purpose and show proof for each installation entry. Providers will furnish verification of a pending Rideshare transaction to Access Control or Directorate of Emergency Services (DES) personnel. Authorized verification methods are:

1. Rideshare providers will display their delivery, fare drop-off or fare pick-up request with their company's application (APP) system. This will include what service is being provided (i.e., food delivery or transportation), a valid destination or address on JBM-HH, the name of the customer, their contact information, and a valid date and time of service not to exceed 30 minutes prior to service(s) requested. JBM-HH DES personnel have the authority to verify the transaction with the customer or Rideshare provider company at any time.

2. Rideshare providers who do not use application-based services to validate their commercial services, are required to have the customer verify their need to access JBM-HH. Rideshare customers are required to contact the JBM-HH Police Dispatch at 703-588-2800 or 703-588-2801 to confirm pending commercial services no more than one hour in advance. The customer must provide the name of the Rideshare company, if applicable, name of the driver, address of service, date and time of transaction, and the customer's name and contact information. JBM-HH DES personnel have the authority to verify the transaction with the customer or Rideshare provider company at any time.

3-10. Trusted Traveler Program (TTP)

a. The TTP allows uniformed service members, spouses, adult dependents, DoD employees, contractors with a CAC, and retired uniformed service members to vouch for passengers in their immediate vehicle, provided the Trusted Traveler vehicle operator possesses a valid DoD affiliated ID card with a Trusted Traveler endorsement token. Vehicle passengers are still subject to 100% identification but are not required to undergo NCIC-III and TSDB vetting.

1. Persons registering for trusted traveler status will register at the VCC.

2. The trusted traveler token and vehicle registration information will be registered in the AIE database.

3. During the registration process, personnel from the VCC will be electronically authenticate that the registrant's driver's license is valid and conduct a NCIC-III check.

4. An electronic approval token is programmed into the authorized TTP sponsor's CAC which is read and verified at installation access control points with AIE enabled equipment.

5. Personnel with trusted traveler enabled tokens must utilize AIE equipped

access control points to utilize the TTP. If a trusted traveler utilizes a non-AIE equipped access gate - 100% vetting IAW paragraph 3-1c is required for the passenger's installation access.

a. The TTP is not authorized for personnel who have AIE passes, dependents 17 years of age and under, or Family Care Providers.

b. Trusted Travelers are entirely responsible for the actions of their passengers and for meeting all local security requirements for escort as established by Army Regulations and the Installation Commander.

c. The TTP procedure is governed and implemented locally and will not be recognized by other installations.

d. Vehicle passengers 10 years of age or older must be in possession of a valid photo ID card (i.e. DL, state ID, DD Form 1173, Uniform Services ID and Privilege card, DD Form 2 series, passport) so they may be readily identified while on JBM-HH.

e. Passengers under the age of 18 who do not possess a valid photo ID card may be vouched for by an authorized adult passenger of the vehicle who has been cleared to enter JBM-HH, IAW paragraph 3-1a of this policy.

f. The TTP will be suspended at FPCONs Charlie and Delta or as directed by the GC.

g. The TTP is not authorized for persons under the age of 18 or persons not in lawful possession of a valid form of identification credentials that do not require a NCIC-III check.

h. The TTP does not authorize vehicle occupants to enter a Mission Essential or Vulnerable Area (MEVA), defense critical asset, task critical asset, limited area, or exclusion area without first meeting the security requirements and procedures for those areas.

i. Trusted travelers cannot vouch for persons with foreign passports or identification cards.

j. A trusted traveler may have their credential revoked at any time. The Trusted Traveler Program is a voluntary program at the direction and discretion of the SC, IAW AR 190-13, Chapter 8.

b. Trusted Traveler Program (TTP). The trusted traveler program is currently not authorized on JBM-HH.

3-11. Debarment

a. The Joint Base Commander may deny a person access for: involvement in the commission of a criminal offense; when access is inconsistent with the interests of National Security; when personal conduct reflects negatively on the image of the United States; or when access adversely affects the health, safety, or morale of persons on JBM-HH.

1. Anyone debarred from JBM-HH may petition the JBC, or their representative, for partial or limited privileges.

2. A Commander’s decision to debar must be based upon investigative evidence, documented facts, and written coordination of the servicing Staff Judge Advocate's (SJA's) office or legal representative when deciding if an incident is serious enough to warrant a debarment.

3. Actions against Civilian employees will be coordinated through the servicing Personnel Office, and such action will be made a part of their official file.

4. Actions to debar contractors from access to JBM-HH will be coordinated with the local Contracting Office.

5. Under certain circumstances, limited debarments may be imposed on person(s) who would otherwise receive debarment from the installation, i.e. persons still requiring access to their place of duty.

6. Debarment information will be entered into the JBM-HH access control system which will have the capability to display debarment status for registered persons.

7. VCC, access control personnel and law enforcement will maintain a list of persons debarred from JBM-HH. All lists are For Official Use Only (FOUO).

8. Local procedures will be used to update lists. Lists will not be released to the public and will be secured in areas that may not be viewed by unauthorized persons.

9. Debarment lists may be combined and maintained in the same manner as lists used for tracking and documenting persons denied on-base driving or other privileges.

10. ACP and VCC personnel will use AIE or local debarment roster to ensure unauthorized persons are denied access, and if applicable, charged with trespassing when entry is illegally gained.

Chapter 4
Commercial Vehicles

4-1. Commercial and Delivery Vehicles

a. Drivers must possess a current bill of lading for the specific delivery containing an address on the installation.

b. Drivers must possess a valid state DL or Commercial Driver’s License (CDL), a state vehicle registration and proof of insurance.

c. All delivery vehicles are subject to a vehicle inspection at any time While on the installation. All delivery drivers must be cleared through NCIC-III. Government sponsors may escort individuals while on the installation in lieu of vetting using NCIC-III.

d. If the vehicle has a seal, the seal's serial number will be checked against the bill of lading to validate authenticity. If the seal is broken or the serial number does not match, a 100% inspection of the vehicle will be conducted.

4-2. Moving Companies

a. Drivers and all occupants must be vetted and have a bill of lading, valid DL, registration, and proof of insurance.

b. Drivers must possess a valid state DL, state vehicle registration, and proof of insurance.

c. All delivery vehicles are subject to a vehicle inspection, and all occupants will be vetted IAW this program.

d. All drivers and occupants must request access and be cleared through NCIC-III. Government sponsor may coordinate with VCC for prior vetting.

4-3. Tow Trucks

a. 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.

1, Virginia Registered Tow Trucks. Drivers will show/display Tow Truck Tag which will either be a "Tow Truck", "Tow Truck Permanent" or "Apportioned" state tag, in order to be utilized for towing vehicles for any type of compensation (compensation includes towing vehicles for automobile repair, transportation as well as repossession purposes. If the Tow Truck doesn't have any of the three types of plates described, it is a Tow Truck which is not authorized for usage by the State for anything other than private use), tow truck Certificate of Vehicle Registration, Driver's License with the Commercial endorsement and Proof of Insurance.

2. Maryland Registered Tow Trucks. Drivers will provide a Collection Agency License from the Office of the Commissioner of Financial Regulation (if the vehicle is operating in a repossession capacity) or a Maryland Transportation Authority Permit (for transportation of vehicles in a non-repossession capacity), Tow Truck Tag which will have the letters "TT" or "TE" in the alphanumeric characters on the MD state tag, tow truck Certificate of Vehicle Registration, Driver's License with the Commercial endorsement and Proof of Insurance.

3. District of Columbia Tow Trucks. Drivers will provide proof of a Repossession License (if the vehicle is operating in a repossession capacity) Which validates the driver/company as licensed as a collection agency with Commerce and Consumer Affairs or Tow Truck Basic Business License (for transportation of vehicles in a non-repossession capacity), Tow Truck Tag which will start with the letter "C" followed by four alphanumeric

characters on the DC tag, tow truck Certificate of Vehicle Registration, Driver's License with the Commercial endorsement and Proof of Insurance.

b. All tow trucks are subject to a vehicle inspection, and all occupants will be vetted IAW this program.

c. Recovery and 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 Desk Supervisor.

2. The Police Desk will provide an escort and notify the Installation Staff Judge Advocate (SJA). The creditor or their agent must provide a copy of title, contract or legal agreement; present evidence that the debtor is in default of the contract or legal agreement; present evidence they are working for the creditor.

3. All drivers are subject to be vetted by NCIC-III prior to entry. Government sponsor will coordinate with VCC for prior vetting. Government sponsors may escort individuals while on the installation in lieu of vetting using NCIC-III.

4-4. Taxi Companies, Transportation Buses

a. Taxi and bus drivers must be cleared through NCIC-III.

1. Drivers must possess a valid state issued DL, valid taxicab operator's license, state vehicle registration, and proof of insurance.

b. Vehicles are subject to inspection before access is granted.

c. Taxi drivers will not be granted access as a trusted traveler.

d. Passengers must possess valid ID and be vetted IAW this program.

4-5. Food Delivery Vehicles and Vendors

a. Vendors and drivers must apply for access and be cleared through NCIC-III.

b. Drivers must possess a valid state issued DL, state vehicle registration and proof of insurance.

c. All vehicles are subject to inspection prior to being granted access.

d. Deliveries must have an on-post destination.

Drivers must apply for access, be cleared through NCIC-III, and have a valid on-post destination.

Chapter 5
ACP Active Vehicle Barrier (AVB) Activation Procedures

5-1 Roles and responsibilities.

a. The Chief of Police oversees policy implementation, SOP enforcement, and training compliance.

b. Watch Commander (WC): Grants authority for bollard activation during suspicious activity, or threat level changes.

c. On-Duty Police/Guard Personnel: Execute bollard activation and deactivation according to the SOP and notify the WC of any irregularities.

d. Physical Security Officer (PSO): Maintains training records, performs system checks, and ensures logs are accurate and complete.

5-2 Procedures.

a. The Pre-Operational Checks (MP, DACP or DASG). At the beginning of each shift, designated personnel will:

1. Conduct a visual inspection of physical damage or obstruction.

2. Test bollard functionality via the control panel.

3. Confirm intercom, CCTV, and communication lines are operational.

4. Log inspection results in the Bollard Operational Logbook.

When to Activate Vehicle Bollards.

b. There are two types of activations for the deployment of the ACP AVBs. The activation procedures are:

1. Routine Activation. The Routine Activation is used during daily operations and testing. Uses of the Routine Activation are:

a. During gate closures at scheduled times.

b. When pedestrian-only access is required (e.g., during special events).

c. During random antiterrorism measures (RAMs).

2. Hot Activation / Emergency Activation. These activations are used during a specific incident that threatens the security of the installation or a breach. Uses of Hot Activation / Emergency Activations are:

a. Upon detection of a Vehicle-Borne Improvised Explosive Device (VBIED) threat.

b. When a vehicle attempts to breach the installation gate without authorization.

c. During installation lockdowns or active shooter scenarios.

d. Officer discretion following JBM-HH Code Red Procedures.

3. Increased Threat Level:

a. When Force Protection Condition (FPCON) is elevated to Bravo, Charlie, or Delta.

b. When suspicious vehicle activity is observed near a critical area.

4. Routine Activation/Deactivation Procedures:

a. Ensure area is clear of personnel and vehicles.

b. Activate bollards using the control panel.

c. Observe confirmation indicator (lights or audible cue).

d. Notify WC of activation and log time, reason, and operator in the Bollard Event Log.

e. Deactivate only when clearance is granted or normal vehicle traffic resumes.

5. Emergency Activation Procedures: (In the event of a threat or breach)

a. Immediately activate bollards via emergency control.

b. Alert the WC and ECC.

c. Monitor and record incidents using CCTV.

d. Submit incident report (DA Form 3975) within 1 hour of event.

6. Manual Operation:

a. If the automated system is non-functional:

b. Use the mechanical override as instructed in the bollard technical manual.

c. Place traffic cones and warning signs in the area.

d. Notify DPW and the WC immediately.

e. Log all actions taken and complete a maintenance request as needed.

7. Post Activation Procedures:

a. Document activation time, duration, and operator in the Bollard Event Log.

b. Review incident on CCTV and file footage for evidence.

c. Conduct post-check to ensure the system is reset and operational.

d. Submit DA Form 1594 (Daily Journal) at end of shift summarizing all bollard related activity.

5-3 Training.

a. All authorized personnel must complete the Bollard Operations and Safety Course annually. A qualified instructor must validate hands-on operation. Quarterly tabletop exercises and biannual practical evaluations will be conducted and logged by the JBM-HH DES Training Division.

5-4 Safety Considerations.

a. Always confirm the area is clear of vehicles, pedestrians, or animals before activating bollards, Use high-visibility signage when bollards are raised, Report any injury or property damage immediately to the safety office and WC, Complete appropriate documentation and witness statements (if applicable).

5-5 Punitive Action.

a. Failure to comply with this SOP may result in disciplinary action, retraining, or revocation of bollard system access privileges as determined by the Director of Emergency Services. Deliberate misuse may result in Uniform Code of Military Justice (UCMJ) or administrative action.

Chapter 6
Limited Use Gates

Approval from the Installation DES is required for access through all limited-use gates, typically reserved for tactical vehicles, construction, HAZMAT, or special events.

a. Henry Gate. Located on JBM-HH at the intersection of Arlington Boulevard and North Pershing Drive. It is used to access JBM-HH for special events and upon special request.

b. Ceremonial Gate. Located on FT McNair at the intersection of P Street Southwest and Third Avenue. It is used to access FT McNair for special events and upon special request.

c. P Street Gate. Located on FT McNair at the intersection of P Street Southwest and Second Street Southwest. It is used to access FT McNair for special events, construction and upon special request.

d. ICAF Gate. Located on FT McNair at the intersection of Fifth Avenue and V Street Southwest. It is used to access FT McNair for special events and upon request.

Appendix A
References

Section I
Required Publications

AD 2011-08, Army Implementation of Homeland Security Presidential Directive-12, 26 May 2011

AD 2014-05. Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors, 7 March 2014

AR 190-5. Motor Vehicle Traffic Supervision, 22 May 2006

AR 190-13. The Army Physical Security Program, 27 Jun 2019

AR 190-14. Arming and The Use Of Force, 01 March 2024

AR 190-16. Physical Security, 31 May 1991

AR 190-51, Security of Unclassified Army Resources (Sensitive and Nonsensitive), 27 June 2019.

AR 190-56. The Army Civilian Police and Security Guard Program, 16 November 2023

AR 380-10. The Conduct and Oversight of the U. S. Army Intelligence Activities, 27 January 2023

AR 380-67. Personnel Security Program, 27 March 2025

AR 525-13. Antiterrorism, 03 December 2019

AR 600-78. Army Suitability, Fitness, and Credentialling Program, 05 March 2024

AR 600-8-14. ID Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel, 21 October 2020

DoD 5200.8-R. Physical Security Program, Incorporating Change 2, 19 October 2020

DoDM 5800.08, Vol 3. Physical Security Program: Access to DoD Installations, Incorporating Change 1, 18 September 2020

DoDI 1000.13, Volume 2. DOD Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals, Incorporating Change 1, 28 July 2020

DoDI 2000.12. DoD Antiterrorism (AT) Program, Incorporating Change 3, 08 May 2017

DoDI 5820.03, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011

DoD Directive-Type Memorandum (DTM) 09-012. Interim Guidance for DoD Physical Access Control, 8 December 2009, Incorporating Change 4, 22 April 2014

HQDA EXORD 033-15. Installation Access (Directed Actions), 7 November 2014

IMCOM OPORD 13-084. Unescorted Installation Access Control for Gold Star Family Members, FRAGO 01, IMCOM Installations, 200030Z March 2015

IMCOM OPORD 15-031. Implement Access Control Procedures at IMCOM Installations,

Homeland Security Presidential Directive-12. Policy for Common Identification Standards for Federal Employees and Contractors, 27 August 2004

JBM-HH Policy Memorandum ES-3. Registration and Control of Privately Owned Weapons, 5 September 2013

JBM-HH Regulation 190-15. Directorate of Emergency Services Uniform Traffic Policy, 16 July 2010

Military District of Washington. Policy Letter - Trusted Traveler Program (TTP), Policy - Memorandum #20, 12 February 2015

Secretary of the Army Memorandum. Uncleared Contractor Common Access Card Credentialing and Installation Access, 31 October 2013

Applicable Federal and State Laws

Appendix B
Acronym
Definitions

AAFES: Army and Air Force Exchange Service
ACP: Access Control Point
ACS: Army Community Service
AD: Army Directive
AF: Air Force (United States Air Force)
AIE: Automated Installation Entry
ALERTS: Army Law Enforcement Reporting and Tracking System
AR: Army Regulation
CAC: Common Access Card
CDC: Child Development Center
CDR: Commander
CIV: Civilian
COPS: Centralized Operations Police Suite
COR: Contracting Officer's Representative
COTR: Contracting Officer's Technical Representative
DA: Department of the Army
DACP: Department of the Army Civilian Police
DASG: Department of the Army Security Guard
DC: District of Columbia
DD: Department of Defense
DES: Directorate of Emergency Services
DL: Driver's License
DoD: Department of Defense
DoDI: Department of Defense Instruction
DPTMS: Directorate of Plans, Training, Mobilization and Security
ENCLS: Enclosures
FBI: Federal Bureau of Investigation
FCP: Family Care Provider
FedEx: Federal Express
FN: Foreign National
FPCON: Force Protection Conditions
GC: Garrison Commander
GOV: Government
HSPD: Homeland Security Presidential Directive
HQDA: Headquarters Department of the Army
IAW: In Accordance With
IC: Installation Commander
ID: Identification
IMCOM: Installation Management Command
INS: Immigration and Naturalization Service
JBC: Joint Base Commander
JBM-HH: Joint Base Myer-Henderson Hall
MD: Maryland
MOW: Military District of Washington
M.I.: Middle Initial
MIL: Military (acronym form – mil – is utilized when it is part of an e-mail address unless otherwise noted)
MP: Military Police
NCIC-111: National Crime Information Center - Interstate Identification Index
NCR: National Capital Region
NLT: Not Later Than
NOAA: National Oceanic and Atmospheric Administration
NTE: Not to Exceed
PAO: Public Affairs Office/Officer
PMO: Provost Marshal's Office
POC: Point of Contact
POV: Privately Owned Vehicle
POW: Privately Owned Weapon
PRB: Personnel Review Board
PS: Physical Security
PSRB: Physical Security Review Board
RAM: Random Antiterrorism Measures
SC: Senior Commander
SECARMY: Secretary of the Army
SE: Special Event
SEP: Special Event Pass
SJA: Staff Judge Advocate
SMC: Senior Mission Commander
SOS: Survivor Outreach Services
TSDB: Terrorist Screening Data Base
TTP: Trusted Traveler Program
UPS: United Parcel Service
US: United States
USA: United States Army
USPS: United States Postal Service
USSS: United States Secret Service
VA: Virginia
VCC: Visitor Control Center
VCIN: Virginia Crime Information Network
VHIC: Veterans Health identification card
VIP: Very Important Person(s)
VSP: Virginia State Police

Appendix C
Joint Base Myer – Henderson Hall Installation Access Request Form 190-16X

Joint Base Myer-Henderson Hall (JBM-HH) Installation Access Request

For use of this form, see JBM-HH Reg 190-16, Proponent is Directorate of Emergency Services

Type of Applicant: *(check appropriate box)*

☐ VISITOR ☐ CONTRACTOR ☐ OTHER

Privacy Act Advisement: The information requested is for the purpose of granting access to the JBM-HH installation. Providing requested information, to include your social security number (SSN), is voluntary. However, your access may not be granted if all requested information is not provided. **Authorities:** Executive Orders (EO) 10450, 10865, and 12333. The SSN, required for record accuracy, is requested pursuant to 10 U.S.C. 3013,
Secretary of the Army; AR 190-13, The Army Physical Security Program, and EO 9397. **Principal Purpose(s):** The information collected on this form is used to screen and identify access applicants to JBM-HH who may have criminal histories or involvements which preclude installation access. Completed forms are used to conduct background records checks for determinations of the eligibility of applicants for access to JBM-HH.
Completed forms are covered by official SORNs. **Disclosure:** Voluntary. However, failure of the applicant to complete any of the applicant required sections may result in refusal of access to JBM-HH. An applicant's SSN is used to conduct law enforcement records checks and Government data base queries. All information is "For Official Use Only" and will only be released to the JBM-HH Police Department or other authorized agency
personnel for the purposes of determining access eligibility and/or enforcing Federal, state, local law or regulations. Information retrieved from law enforcement records checks and Government data base queries will not be disclosed to the applicant IAW National Crime Information Center and Interstate Identification Index laws, user agreements, Army Directive 2014-05 and official guidance.

Section A. Visitor Applicant Information

1. Name *(last, first, middle initial):*	2. Date of Birth:	3. Gender: ☐ Male ☐ Female	4. Race:

5. Social Security Number:	6a. Driver's License or State ID Number:	6b. Issuing State or Territory:	6c. U.S. or U.S Territory Passport Number (*if state driver's license or ID not available):*

7. Residential Address: *(Include City/State/ZIP Code)*	8. Home Phone Number:	9. Cellular Phone Number:

10. Are you a U.S. Citizen? ☐ Yes ☐ No

If you are a U.S. Citizen, skip questions 10a thru 10d

10a. Do you have a Visa, Foreign Passport or Official Military Orders allowing travel, work or residency in the U.S.? ☐ Yes ☐ No

Please indicate what documentation you have and the corresponding alphanumeric number: _____

10b. ☐ **Work Authorization Card (aka; Employment Authorization Card): Form I-766** ☐ **Permanent Resident Card (aka; Green Card): Form I-551**

List the alphanumeric identifier for your work authorization document: _____

10c. Do you have a Alien Registration Number (ARN): ☐ Yes ☐ No

(If yes, list your ARN: _____)

10d. Do you have a Foreign National Number (FNN): ☐ Yes ☐ No

(If yes, list your FNN: _____)

Note: If you are a non-U.S. citizen, you must provide all relevant documentation for verification. The visitor Control Center (VCC) is required to make and retain photocopies of all docu- mentation which allows you to work, reside or visit the U.S. for the purpose of installation access.

11. Applicant Category: *Please place a check beside the description which best describes your category.*

☐ Non-DoD Affiliate Visitor ☐ Gold Start Family Member ☐ Foreign Military Member on Official Orders ☐ Taxi/Limo/Uber or Lift Driver ☐ Foreign National Family Care Provider ☐ Employee of JBM-HH Resident ☐ Volunteer ☐ Tow Truck Driver ☐ Commercial Delivery ☐ Moving Company

☐ Guest of JBM-HH Resident ☐ DRMWR Member ☐ Event Attendee ☐ Thrift Shop ☐ Other _____

12. Requested Duration of Access: (not to exceed 1 year) *Requested Date(s)/Time(s) of Visit*	13. Justification for Pass:
From Date: _____ To Date: _____ From Time: _____ To Time: _____	

Section B. Contractor/Vendor Information (If Applicable)

1. Contractor/Vendor Company Name:	2. Company Phone Number:	3. Contract Number: *(if applicable)*

4. Contractor/Vendor Address: *(Include City/State/ZIP Code)*	5. Contractor/Vendor Company Point of Contact:

6. Contractor/Vendor Applicant Category: *Place a check beside the description which best describes your contract category.* ☐ CAC eligible Contractor ☐ Non-CAC eligible Contractor	7. Requested Duration of Access: *(Not to exceed one year)*	8. Contract Dates and Work to Be Performed:

JOINT BASE MYER-HENDERSON HALL
ACCESS CONTROL WAIVER APPLICATION

For use of this form, see JBM-HH Reg 190-16; Proponent is Director of Emergency Services

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

PRIVACY ACT ADVISEMENT: The information requested is for the purpose of granting access to the Joint Base Myer-Henderson Hall (JBM-HH) Installation. Providing requested information, to include your social security number (SSN), is voluntary. However, your access may not be granted if all requested information is not provided. AUTHORITIES: Executive Orders (EO) 10450, 10865, and 12333. The SSN, required for record accuracy, is requested pursuant to 10 U.S.C. 3013, Secretary of the Army; AR 190-13, The Army Physical Security Program; EO 9397 (SSN).

PRINCIPAL PURPOSE(S): The information collected on this form is used to screen and identify access applicants to JBM-HH who may have criminal histories or involvements which preclude installation access. Completed forms are used to conduct background records checks for determinations of the eligibility of applicants for access to JBM-HH. Completed forms are covered by official SORNs.

DISCLOSURE: Voluntary. However, failure of the applicant to complete any of the applicant required sections may result in refusal of access to JBM-HH. An applicant's SSN is used to conduct law enforcement record checks and Government data base queries. All information is "For Official Use Only" and will only be released to the JBM-HH Police Department or other authorized agency personnel for the purposes of determining access eligibility and/or enforcing Federal, state, local law or regulations. Information retrieved from law enforcement record checks and Government data base queries will not be disclosed to the applicant IAW National Crime Information Center and Interstate Identification Index laws, user agreements, Army Directive 2014-05 and official guidance.

1. Name *(First/Middle/Last/Suffix)*:

2. Current Address *(Number and Street, City, State, and ZIP Code)*:

3. Email Address:

*Do you want your decision *emailed back to you rather than mailed to you?* ☐ *Yes* ☐ *No*

***Please note**: JBM-HH is committed to protecting all Personally Identifiable Information (PII). JBM-HH recommends the use of postal delivery to ensure dissemination to authorized persons, the protection of PII and verification of the intended receiver via certified United States Postal Service signature receipt. Should you prefer to receive determination decisions by electronic communication, JBM-HH cannot authenticate a recipient's identity thereby ensuring confidentiality. Additionally, JBM-HH cannot verify receipt of the determination. If the e-mail option is selected as the delivery method, the applicant accepts any and all risks of system(s) or server(s) failures etc., which may impede delivery beyond the control of JBM-HH or access to the determination by other parties with legal or illegal access to the intended recipient's e-mail account. The applicant further certifies, if selecting e-mail notice, proper notification has been made once JBM-HH transmits the determination via electronic delivery. JBM-HH will retain a copy of the sent e-mail, time and date stamped, as verification. E-mail notification is a risk the applicant undertakes with the knowledge that the above items cannot be assured by JBM-HH or refuted by the applicant at a future date.*

4. Phone Numbers:

4a. Home:	**4b. Work:**	**4c. Cell:**

5. Reason for Requesting Access to JBM-HH:

6. If installation access is for employment, what job was JBM-HH offered you?

7. Does your job require you to have a security clearance of any type? If so, please state which type of clearance is required.

8. List your entire criminal history (except minor traffic infractions) as follows:			
8a. Crime for which you were arrested	**8b. Crime for which you were convicted (or indicate if dismissed or null pros)**	**8c. Name and Address of court of agency**	**8d. Disposition (include sentence and conviction date)**

9. Attach a copy of your Identity History Summary Check and/or Criminal History Record, all required documents listed in the instructions, any court documents, CERTIFIED by the Clerk of the Court from all of your conviction(s), arrests or charges. Copies will only be accepted if certified as copies of originals by a NOTARY PUBLIC.

10. In your own words, explain the facts of each arrest and conviction, and why you should be able to come on post. The following areas must be addressed for each incident: the nature and seriousness of the conduct, the specific circumstances surrounding the conduct, the length of time elapsed since the conduct, the age of the individual at the time of the incident/conduct and any proof of efforts towards rehabilitation. Attach additional sheets if necessary.

11. Explain any special or specific circumstances that require access to JBM-HH. Attach additional sheets if necessary.

12. Have you been denied access by any other federal organization? (*please check*) ☐ **Yes** ☐ **No**
If yes, indicate the reason for the denial.

13. List all references that you would like the PRB to consider on your behalf. Include name, address, telephone number, and relationship. By listing references and signing this waiver request, you authorize JBM-HH PRB to contact the below listed references for character questions.

14. Attach any additional sheets, numbered to the related section, if necessary.

15. 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 E

JBM-HH Installation Support Request Form-7

Joint Base Myer-Henderson Hall Installation Support Request Form

For use of this form, see JBM-HH Policy Memo PL-2; proponent is Directorate of Operations

FOR OFFICIAL USE ONLY

Information provided for this form may include Operational Security and/or Law Enforcement Sensitive Data and shall be protected from non-mandatory disclosure.

Questions: call (703) 696-5113 / 5662 / 3290 / 3291
Once filled out, email to: usarmy.jbmhh.id-sustainment.mbx.dptms-bdoc@army.mil (in Global as "USARMY JBM-HH ID-Sustainment Mailbox DPTMS-BDOC")

SECTION I – CONTACT INFORMATION

1. Organization:
2. Military Sponsorship: N/A
3. Point-of-Contact:
4. Email:
5. Telephone:
6. Date Submitted/Received:

SECTION II – EVENT DESCRIPTION

7. Who is Putting on the Event:
8. What is the Event:
9. Date/Time of Event (for setup/teardown purposes):
10. Location of Event:
11. Reason for Event:
12. Number of Expected Guests:
13. Number of VIPs and Names (attach additional sheets, if needed):

SECTION III – SUPPORT REQUESTED

14. Summary of Support Requested (be as specific as possible; use additional sheets, if needed):

DIRECTORATE OF OPERATIONS USE ONLY

Action Officer	
Date Request Received	
Is This a Reimbursable Event?	
Date Support Confirmed	
Date Confirmation Sent to POC	

Appendix F

Fitness Determination Evaluation Guide

Administrative / Legal Actions			
Inability to verify claimed identity and/or submitted fraudulent identity information	**DENY**		
Currently barred from any Federal installation or facility	**DENY**		
Active wants or warrants	**DENY (See para 6-2, j)**		
Any charge with an unknown disposition which would otherwise result in a denial determination if the disposition was conviction.	**DENY**		
Knowingly/willfully engaged in acts or activities to overthrow the U.S. Government by force in any jurisdiction or any country; or conspiracy or attempt to commit offense.	**DENY**		
Known/suspected terrorist or belongs to known/suspected terrorist organization	**DENY**		
Registered Sex Offender	**DENY**		
CRIMINAL HISTORY - CONVICTIONS	**< 5 YEARS**	**< 10 YEARS**	**> 10 YEARS**
Felony conviction for child abuse involving serious bodily injury to a child or minor	**DENY**	**DENY**	**ALLOW**
Felony conviction for armed robbery or conspiracy or attempt to commit offense	**DENY**	**DENY**	**ALLOW**
Felony conviction for kidnapping or hostage taking	**DENY**	**DENY**	**ALLOW**
Felony conviction involving distribution, sale, use, possession, or manufacture of an explosive, explosive device, or firearm; or conspiracy or attempt to commit offense	**DENY**	**DENY**	**ALLOW**
Felony conviction for mayhem, maiming, manslaughter, or negligent homicide	**DENY**	**DENY**	**ALLOW**
Felony conviction for any type of extortion, bribery, or fraud	**DENY**	**DENY**	**ALLOW**
Felony conviction for importation or manufacture of a controlled substance	**DENY**	**DENY**	**ALLOW**
Felony conviction for any type of burglary or robbery	**DENY**	**DENY**	**ALLOW**
Felony conviction for any type of possession or distribution of stolen property	**DENY**	**DENY**	**ALLOW**
Felony conviction for any type of threat or disruption to the public (terroristic threat, inciting a riot, etc.)	**DENY**	**DENY**	**ALLOW**
Felony conviction for any type or arson (degree charge based)	**DENY**	**DENY**	**ALLOW**
Felony conviction for any type of assault (degree charge based)	**DENY**	**DENY**	**ALLOW**
Felony conviction not listed above	**DENY**	**DENY**	**ALLOW**
Conviction for murder or conspiracy or attemptto commit offense	**DENY**	**DENY**	**DENY**
Kidnapping, hostage taking, human trafficking, or human smuggling; or conspiracy or attempt to commit offense	**DENY**	**DENY**	**DENY**
Rape, forcible sodomy, or sexual assault: or conspiracy or attempt to commit offense	**DENY**	**DENY**	**DENY**
Any sexual offense invoving a minor or child, including child molestation or child pornography; or conspiracy or attempt to commit offense	**DENY**	**DENY**	**DENY**
Distribution of, or possession with intent to distribute a controlled usbstance; or conspiracy or attempt o commit offense	**DENY**	**DENY**	**DENY**
Conviction for espionage, sabotage, treason, or terrorism (Not Terrorist Threats); or conspiracy or attempt to commit offense	**DENY**	**DENY**	**DENY**
Three (3) or more convictions for operation of a motor vehicle while intoxicated by alcohol or drugs in any jurisdiction in the last 5 years	**DENY**	**ALLOW**	**ALLOW**
Six (6) or more convictions of misdemeanor criminal offenses within thE last 5 years; excluding moving violations	**DENY**	**ALLOW**	**ALLOW**
LEGEND			
No discretion on waiver packet issuance; visitors denied access will be issued an access denial waiver packet. Visitor may be escorted IAW paragraph 3-4	**DENY**		