UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

MCIEAST-MCB CAMLEJO 5530.15B
G-3/5
FEB 10 2020

MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE CAMP LEJEUNE ORDER 5530.15B

From: Commanding General
To: Distribution List

Subj: REGIONAL ACCESS CONTROL REGULATIONS

Ref: (a) DoDM 5200.08 Vol 3, "Physical Security Program: Access to DoD Installations," of January 2, 2019
(b) MCO 5580.2B Ch 2
(c) MCO 5512.11E
(d) MCO 5580.1C
(e) DoD 5400.11-R, "Department of Defense Privacy Program," of May 14, 2007
(f) MCO 1740.13D
(g) MCO 11000.22 Ch 1
(h) CG MCIEAST-MCB Policy Letter 13-19
(i) John S. McCain National Defense Authorization Act for Fiscal Year 2019 of 13 August 2018

Encl: (1) Regional Access Control Regulations

1. Situation. Base and Station Commanders conditionally grant the privilege to gain access to their respective Installation to those individuals or organizations that meet the minimum qualifications and conform to regulations contained in this Order and references (a) through (i). If someone breaches the terms of this Order or the references, the Installation Commander may suspend or revoke the privilege to access their respective Installation.

2. Cancellation. MCIEAST-MCB CAMLEJO 5530.15A.

3. Mission

a. Marine Corps Installations East (MCIEAST) publishes direction to ensure common minimum standards and unifying procedures to govern installation access policy throughout MCIEAST and across all component installations. Installation commanders will publish and enforce local access control policy that meet or exceed the minimum acceptable standards detailed in this Order.

b. This Order establishes the minimum criteria and procedures for access to MCIEAST Installations to promote the readiness, sustainment, and quality of life of the Marines and their families, as well as other military forces and tenant commands personnel. It also establishes roles, responsibilities, regulations, and consequences for

individuals who violate this Order. This Order is applicable to all military and civilian personnel, family members, contractors, and any other individual or organization desiring to gain access to any MCIEAST Installation. Individuals who violate the provisions of this Order are subject to administrative action or criminal prosecution.

c. Summary of Revision. This Order was revised to incorporate updates promulgated by higher headquarters directives. This Order should be thoroughly reviewed in its entirety.

4. Execution

a. Commander's Intent. MCIEAST Installations will publish and enforce access control policy that is consistent in terms of minimum standards, but also tailored to meet the specific conditions, which prevail at each individual installation.

b. Concept of Operations. Individual installation commanders will adopt the minimum access standards identified in this document and will use them as foundation on which to build local, installation specific, access policy. These local access policies will be tailored to fit local circumstances, but will, because of the common foundation, be generally consistent with the procedures in force at other MCIEAST Installations.

5. Administration and Logistics. This Order has been coordinated with and concurred by the Commanding Generals, II Marine Expeditionary Force, Commander, U.S. Marine Corps Forces Special Operations Command, and U.S. Marine Corps Logistics Command. For the purposes of this Order, MCIEAST Installations refers to Marine Corps Base Camp Lejeune, Marine Corps Air Station (MCAS) New River, MCAS Cherry Point and outlying airfields, MCAS Beaufort, Marine Corps Logistics Base Albany, and Marine Corps Support Facility Blount Island.

6. Command and Signal

a. Command. This Order is applicable to all MCIEAST Installations and subordinate and tenant commands aboard these Installations.

b. Signal. This Order is effective the date signed.

N. E. DAVIS
Chief of Staff

DISTRIBUTION: A/B/C

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

TABLE OF CONTENTS

Chapter 1

Introduction

1. General

a. This Order is primarily designed to improve security through a combination of policy and process changes pertaining to base access while implementing updated requirements identified references (a) through (i). This Order establishes a set of common core, unifying principles, and minimum standards and procedures, to guide the development and implementation of installation policy. Nothing in this Order relieves the commander from the responsibility or authority to ensure the security and efficient operation of their installation.

b. Entry onto MCIEAST Installations is a privilege, not a right. Individuals entering MCIEAST Installations must have an acceptable purpose for access. This includes uniformed military personnel, family members, Department of Defense (DoD) civilian employees, unaffiliated civilians, DoD and other authorized contractors, and other authorized patrons.

2. Objectives. This Order is designed to enhance security and mitigate unauthorized personnel from accessing MCIEAST Installations.

3. Description of Operations and Key Concepts

a. All individuals seeking access to MCIEAST Installations will be screened in accordance with the process and standards detailed in this Order and the access control policy of the concerned installation. Individuals who pass screening will be issued an appropriate credential (a credential for long-term access, or a temporary pass for one time or short-term access) and allowed to access the installation.

b. The technical enabler and enterprise wide solution for Electronic Physical Access Control System (EPACS) at all MCIEAST Installations is the Defense Biometrics Identification System (DBIDS). The DBIDS EPACS is used to screen applicants, issue credentials or temporary passes, and manage the access of approved personnel. Refer to Chapter 7 for further details on EPACS and DBIDS.

c. The intent of the DBIDS credential and DBIDS temporary pass is the issuance of a credential that indicates the identity of the individual, and any limitations of access granted. The DBIDS credential must remain in the possession of the individual, is property of the U.S. Government, is not transferable, and must be presented or surrendered upon demand to any Installation security

official, or whenever challenged by Installation personnel. The DBIDS credential and temporary pass are the property of the U.S. Government and must be surrendered to the Installation when no longer required for access.

d. Personnel will be denied access if they are unable to meet the access control requirements for the types of access outlined in this Order.

e. Nothing in this Order is to be construed as limiting the Commanders' authority to maintain a secure Installation.

f. This Order is a punitive, lawful general order. Any violation, attempted violation, or solicitation of another to violate the provisions set forth in this Order is punishable under the Uniform Code of Military Justice (UCMJ) for uniformed service members, is the basis for disciplinary action with respect to civilian employees, and subjects all violators to criminal prosecution under applicable state or Federal law.

4. Types of Authorized Access. The three types of authorized access to MCIEAST Installations are unescorted, escorted, and trusted traveler.

a. Unescorted Access. Unescorted access requires individuals to establish their identity, be determined fit for access, and establish an acceptable purpose for presence on the installation.

b. Trusted Traveler Access. Trusted Traveler access allows for the following:

(1) Authorized individuals who have been granted unescorted access, who possess a valid Common Access Card (CAC), or a Uniformed Services Identification Card (USID), and is over age 16, to simultaneously vouch for co-travelers (in the same vehicle or on foot) and enable those co-travelers to obtain trusted traveler access.

(2) All personnel acting in a Trusted Traveler capacity are responsible for the conduct of each sponsored guest and must ensure each guest remains with the Trusted Traveler for the duration of the guests' visit. A violation, attempted violation, or solicitation of another to violate the Trusted Traveler Program requirements, including sponsorship of guests failing to meet installation access requirements may subject all involved to adverse administrative and/or punitive action.

(3) The number of co-travelers may not exceed five individuals per trusted traveler unless specifically authorized by the Installation commander.

(4) Individuals using a non-CAC local or regional DoD credential (DBIDS), Federal PIV, and Non-Federal PIV I, or any other form of identification do not qualify as Trusted Travelers in accordance with this Order. Non-Trusted Travelers granted unescorted access to MCIEAST Installations will not be permitted to sponsor guests. Any individual accompanying a non-trusted traveler must establish a valid purpose to enter the installation, have their identity verified, and establish historic and current fitness prior to being granted access.

(5) The trusted traveler program is permitted for site access only during the hours of 0530 to 2000. Between the hours of 2000 to 0530 all occupants, over the age of 18, must present an acceptable credential to access control point (ACP) personnel. Commanders are authorized to suspend trusted traveler programs at any time based on local conditions.

c. Escorted Access. Persons unable to meet the requirements for unescorted access may be granted escorted access. Escorts must: be provided by the organization or otherwise associated with the visit; must remain within reasonable visual contact of the individual; must report any conduct by the escorted person that causes risk to safety, security, or efficiency; must be U.S. citizens; have a DoD affiliation; and themselves be granted unescorted access in accordance with reference (a).

Chapter 2

Roles and Responsibilities

1. Installation Commanders

a. Shall establish specific policies and procedures for access control consistent with the minimum standards and procedures in this Order and the mandates established in references (a) through (i).

b. Shall closely supervise the implementation of the local installation access policy to ensure that intended results are achieved.

c. Shall identify fiscal, training, and technological shortfalls which significantly interfere with abilities to meet access control requirements.

d. Shall periodically reevaluate the specific policies and procedures in a local installation access order to ensure that they remain relevant and adequate to the intended purpose.

e. Shall ensure Trusted Traveler privileges are suspended in Force Protection Condition (FPCON) CHARLIE and DELTA.

f. Shall define the parameters for commercial vehicle inspections in the respective installation access control policy.

2. Provost Marshal's Office (PMO)/Marine Corps Police Department (MCPD)

a. Shall develop and recommend specific policies and procedures consistent with the minimum standards and procedures found in this Order, the installation access policy, and the mandates established in references (a) through (i).

b. Are responsible to establish and maintain the enforcement infrastructure necessary to execute the requirements of this Order, to include staffing, training, equipment, Standing Operating Procedures, etc, in accordance with reference (b).

c. Are responsible for the daily execution of the access control requirements.

d. Shall ensure only authorized personnel perform access control duties to include vetting, authorizing access, and/or denying access.

e. Shall constantly evaluate and assess all aspects of access control capabilities and functionality in order to enhance efficiency and productivity.

3. Communication Strategy and Operations (COMMSTRAT). The Installations COMMSTRAT will publish press releases/media advisories concerning access control policy changes through appropriate sources.

4. Installation Protection (IP). The Installations' Mission Assurance or IP Branch, and the Naval Criminal Investigative Service (NCIS) will provide threat assessments and updates to the Installation PMOs/MCPDs as directed by current orders and directives.

Chapter 3

Standards for Identity Proofing, Vetting, and Authorized Identification

1. Identity Proofing and Vetting. Access control standards will include establishing identity, historical and current fitness, and acceptable purpose for entry.

a. Non-Federal government and non-DoD-issued cardholders who are provided unescorted access must undergo identity proofing and vetting to determine eligibility for access. Identity is established by presenting one acceptable credential or combination of source identity documents identified in reference (a). Vetting is completed when historic and current fitness has been established in accordance with reference (a). The Visitor Center Office (VCO) or Contractor Vetting Office (CVO) will issue a DBIDS credential to non-Federal government and non-DoD personnel who require extended (over 60 days) unescorted access to the Installation for official government business, but do not require access to government computerized systems. Further, the VCO or CVO will issue a temporary pass (60 days or less) to non-Federal government and non-DoD personnel who require unescorted access to the Installation for official government business, but do not require access to government computerized systems.

b. Federal PIV and DoD issued card holders require only screening for current fitness prior to gaining access to MCIEAST Installations.

(1) Individuals possessing a DoD issued CAC are vetted to DoD personnel security standards and will be considered identity proofed and meet historic fitness as set forth in reference (a).

(2) Individuals possessing Federal PIV credentials that conform to reference (c) are vetted and adjudicated by government security specialists on National Agency Check with Inquiries (NACI) or Office of Personnel Management (OPM) Tier I standards, and will be considered identity proofed and meet historic fitness as set forth in reference (a).

(3) The Transportation Worker Identification Card (TWIC) holders' process of vetting, adjudication, and issuance is comparable to the NACI and OPM Tier I standards, and will be considered identity proofed only, in accordance reference (a). These individuals require vetting for historic and current fitness prior to the issuance of any DBIDS credential or DBIDS temporary pass.

(4) Vetting and adjudication for individuals receiving government ID credentials as listed in reference (a), occur prior to permanent card issuance. Individuals in possession of these ID cards and/or credentials will be considered vetted for unescorted access.

c. Non-Federal government and non-DoD issued card holders provided unescorted access require identity proofing and vetting to determine eligibility for access.

(1) Individuals requesting access will provide an acceptable purpose to enter MCIEAST Installations.

(2) Individuals requesting access not in possession of an approved, government issued card, will provide the documents listed in chapter 3, paragraphs 7(d) through 7(l) of this Order. An authorized PMO/MCPD representative will review the documents presented for the purposes of identity proofing.

(3) Installation Commanders must conduct reoccurring historic fitness checks annually of all personnel issued a DBIDS credential, or a locally produced credential if the installation was granted a deviation in accordance with reference (a). However, Installation Commanders may increase the frequency for historic fitness checks based upon the local security posture if deemed necessary.

(4) Only personnel delegated by the Provost Marshal/Police Chief perform access control duties, to include vetting, authorizing access, or denying access.

(5) Identity proofing and vetting of persons requiring access to the Installation must be conducted by querying data sources to validate and verify the claimed identity of the individual. PMO/MCPD will also determine access eligibility by using biographical information. This information may include, but is not limited to, the person’s name, date of birth, and social security number.

(6) In accordance with references (a), (d), and (e) Installation PMOs/MCPDs personnel will query the following government authoritative data sources to vet the claimed identity and determine historic and current fitness using biographical information including, but not limited to, the person’s name, date of birth, and social security number:

(a) The National Crime Information Center (NCIC) Database;

(b) The Interstate Identification Index (III);

(c) Terrorism lists, such as the NCIC Known and Appropriately Suspected Terrorist (KST) file and the Terrorism Screening Database (TSDB);

(d) Felony wants and warrants, such as those listed in the NCIC Wanted Persons File;

(e) Barment order lists, such as relevant service criminal justice information systems;

(f) Other relevant government databases that may be available such as:

1. Other NCIC files (including the National Sex Offender Registry);

2. Criminal justice or immigration databases; or

3. Other appropriate biometric or biographic government databases

(g) Other sources as determined by the DoD component or Installation Commander. These can include but are not limited to:

1. Department of Homeland Security (DHS) E-Verify;

2. DHS U.S. Visitor and Immigrant Status Indicator Technology;

3. Department of State Consular Checks (non-U.S. citizen); and

4. The Foreign Visitor System-Confirmation Module.

2. Access. Individuals possessing more than one acceptable credential must use the credential specific to the purpose for visiting the installation.

a. All visitors requesting unescorted access must be appropriately sponsored through the VCO or CVO. These individuals will have an acceptable purpose for accessing the installation, per reference (a).

b. Any person in legal possession of a DoD issued CAC that requests entry onto an installation will be granted access unless other circumstances exist that lead access control sentries to believe further identity proofing, fitness determination, or acceptable purpose verification is needed. In those cases, the vehicle, driver, and occupants may be sent to the Installation VCO or inspection site for further review.

c. All non-CAC/non-DoD ID card issued visitors will report to the VCO or CVO to be identity proofed and vetted before the issuance of a DBIDS credential or DBIDS Temporary Pass.

d. Non-governmental delivery personnel and non-regularly scheduled deliveries will report to the designated location determined by the local installation for identity proofing and determination of fitness for access. Once fitness is determined, a DBIDS temporary pass will be issued and the individual must proceed to the designated inspection site for a vehicle inspection prior to gaining access to the installation, per local policy.

e. Non-governmental delivery companies who frequently deliver aboard MCIEAST Installations may be vetted prior to accessing the Installation and issued a DBIDS credential or DBIDS temporary pass. The issuance of a credential or temporary pass does not negate the requirement for a vehicle inspection each time the individual accesses the installation, per local policy.

f. Public-Private Venture (PPV) housing residents who do not possess an authorized CAC are required to sponsor their housing guests in person at the Installation VCO or CVO. All guests shall have their identity established, fitness determined, and be issued a DBIDS temporary pass in accordance with this Order and other applicable directives prior to entry.

g. Designated caregivers, in accordance with reference (f), shall follow local instructions for access to obtain a DBIDS credential or DBIDS temporary pass to the Installation. The caregiver shall maintain a copy of documentation provided by the Installation Commander, or designee, on their person when accessing an MCIEAST Installation, and at all times while aboard the Installation.

h. Divorced non-military affiliated parents or legal guardians of minor dependent children that need access to a MCIEAST Installation for medical care, pharmacy services, etc., may present themselves at the Installation VCO to obtain a DBIDS credential or DBIDS temporary pass. They must present the child's DoD issued identification and official documentation identifying them as the legal parent or guardian of the child, have their identity established and fitness determined prior to being granted access.

3. Denial of Access. Persons requesting access to Marine Corps sites will be denied access if:

a. Military or civilian police or VCO/CVO personnel are unable to verify the individual’s claimed identity based on reasonable belief the person submitted fraudulent identity information in the attempt to gain access.

b. The individual has a conviction for espionage, sabotage, sedition, treason, terrorism, armed robbery, or murder.

c. The individual has a felony conviction for a firearms or explosives violation, regardless of the date of conviction.

d. The individual has been convicted of crimes encompassing sexual assault or rape.

e. The individual has been convicted of crime encompassing child molestation, or the possession or production of child pornography.

f. The individual has been convicted of trafficking in persons.

g. The individual is a registered sex offender.

h. The individual has been convicted of drug possession with intent to sell or distribute.

i. The individual has an active arrest warrant from Federal, state, local, or other civil law enforcement authorities, regardless of offense or violation.

j. The individual has a felony conviction within the last 10 years, regardless of the offense or violation.

k. The individual's name appears on any Federal or state agency watch list for criminal behavior or terrorist activity.

l. The individual is debarred entry or access to a Marine Corps site, other DoD installations or facilities, or other Federal site or facility.

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

n. The individual is known to be or reasonably suspected of being a terrorist or belongs to an organization with known terrorism links/support.

o. The individual is identified in the NCIC KST file, or the TSDB report 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. If an individual is identified on the NCIC KST files or TSDB, PMO/MCPD or other designated site security personnel will immediately call the NCIS Multiple Threat Alert Center (MTAC) for further coordination. The MTAC will coordinate with the Department of Justice or Federal Bureau of Investigation and provide handling instructions to PMO/MCPD or other designated site security personnel.

p. Illegally present in the U.S.;

q. Has knowingly submitted an employment questionnaire with false or fraudulent information;

r. A prisoner on a work-release program or currently on felony probation/parole;

s. Is pending any felony charge;

t. Has been convicted of three or more misdemeanor violations, or attempted violations, within the previous 10 years of the following offenses:

(1) Sex crimes;

(2) Assaults;

(3) Larcenies;

(4) Drugs; or

(5) Weapons.

u. The individual has criminal arrest information that the site commander determines the person presents a threat to the good order, discipline, or health and safety on the Marine Corps site.

v. Any reason the Installation Commander deems reasonable for good order and discipline.

4. Grandfather Clause. Any individual who has been issued access credentials based on previous guidance and have no recent pending charges or convictions will not be penalized as a result of this Order when they renew their access control credentials.

5. Appeals. All personnel who are denied access may appeal to the Installation Commander or appointed designee in accordance with Reference (a) and local policy. PMOs/MCPDs will provide a record of all previous criminal convictions to the deciding official as part of the appeal process. Installation commanders must and shall conspicuously post the adjudication criteria and redress and appeal process, at the site VCO/CVO and World Wide Web site for those negatively adjudicated.

6. Acceptable Credentials

a. Visitors and contractors must provide a valid, original form of ID from those listed in paragraph 7 of this chapter for the purpose of identity proofing for issuance of a DBIDS credential or DBIDS temporary pass.

b. Prior to acceptance, personnel processing an applicant will screen documents for evidence of tampering, counterfeiting, or other alteration. Documents that appear questionable (i.e., having damaged laminates) or otherwise altered will not be accepted. Altered documents will be held until appropriate authorities are notified and disposition procedures are conducted.

7. Acceptable Identity Source Documents. All documents must be original and current.

a. DoD CAC. The CAC simultaneously establishes identity, historic fitness, and purpose.

b. DoD USID. The USID establishes identity and generally establishes purpose.

c. Non-CAC LRC (DBIDS credential) issued by the local installation. These credentials simultaneously establish identity, historic fitness, and purpose for the installation in which they were issued. Individuals requiring multiple installation access to MCIEAST Installations must present themselves at each installation and provide an acceptable purpose to be granted unescorted access to each installation.

d. REAL ID compliant driver’s license or REAL ID compliant non-driver’s identification card issued by a state, territory, possession, or the District of Columbia. These credentials establish only identity.

e. Enhanced driver’s license issued by a state, territory, possession, or the District of Columbia. These credentials establish only identity.

f. U.S. passport or passport card. These credentials establish only identity.

g. Foreign passport bearing an unexpired immigrant or non-immigrant visa or entry stamp. These credentials establish only identity.

h. Any other U.S. Federal, state, territory, possession, or District of Columbia Government-issued credential bearing a photograph, including credentials from other paragraphs in this section, deemed acceptable by the DoD Component head and consistent with applicable laws.

i. Federal PIV card. The PIV simultaneously establishes identity and historic fitness.

j. Veteran's Health Identification Card (VHIC). The VHIC simultaneously establishes identity and purpose. Any individual accompanying the VHIC holder must be vetted for determination of fitness and issued a DBIDS temporary pass.

k. Non-Federal PIV-interoperable (PIV-I) card. The PIV-I establishes only identity.

l. The TWIC establishes only identity.

m. MCIEAST Installations will also accept an original or certified true copy of a birth certificate bearing a raised seal and social security card in conjunction with a non-Real ID compliant driver's license or state issued identification card. In the event this combination identity documents are used, all three must contain the same name or the individual must provide legal documentation such as a court order, marriage certificate, or divorce decree.

n. Individuals under the age of 18 who are unable to present a document listed above must be sponsored by an adult with the proper identification listed in paragraph 7.

o. Children under the age of 16 residing aboard MCIEAST Installations may only sponsor a visitor with the approval of the children's legal guardian. For example, a 12 year old dependent child residing aboard the Installation cannot use their valid dependent DoD ID Card to vouch for their grandparent (having no other military affiliation) aboard the Installation. In this instance, the grandparent must be identity proofed, vetted, and obtain a DBIDS temporary pass for unescorted access prior to accessing the installation.

Chapter 4

Standards of Admittance

1. Entrances and Exits

a. Only personnel assigned to the PMO/MCPD will guard active ACPs to MCIEAST Installations.

b. Motorists must enter and exit on designated roads unless otherwise authorized by the Installation Commander. Any deviation from authorized entrances and exits must be coordinated with the PMO/MCPD.

2. Admittance of Motor Vehicles (MVs)

a. To the greatest extent possible, Federal, state, county, and city owned vehicles will be admitted without unnecessary delay. Despite the goal of preventing unnecessary delay, these vehicles are subject to search, vehicle and driver identity proofing and vetting as prescribed in local policy, and other procedures necessary to maintain safety and security aboard the Installation.

b. Non-registered off-road recreational vehicles are defined as those vehicles that cannot be registered for use on paved roads. This definition generally includes vehicles such as three and four wheeled all-terrain vehicles (ATVs), dirt or trail bikes, dune buggies, and go-carts. These vehicles are only authorized for use in designated areas as defined by local policy.

c. Students attending an entry-level service school must have written authorization from the School Director to register a personally owned vehicle (POV) and will follow the guidelines in this Order.

d. This Order prohibits any individual (military, civilian, retirees, contractors, etc.) from knowingly entering any area within an Installation and operating a MV while the registered owner’s Installation driving privileges are either suspended or revoked, unless that individual is a spouse or dependent of the registered owner.

e. Owners are prohibited from displaying on their MVs in any format any of the following: flags, signs, posters, bumper stickers, window decals, art, emblems, insignia, or other adornments of an extremist, indecent, sexist, racist, obscene, profane, or defamatory nature; other messages that are prejudicial to good order and discipline or otherwise violate the standard of decency found in Article 134 (Indecent Language) of the UCMJ, display a clear danger to the loyalty, discipline, or morale of military personnel, or presents

a potential for disruptive conduct and interference with the mission of the command. The unauthorized display of any such flag, sign, poster, bumper sticker, window decal, art, emblem, insignia, or other adornments may be grounds for suspension or revocation of Installation driving privileges or denial of access to the Installation. The Staff Judge Advocate (SJA) for each Installation will review, on a case-by-case basis, any suspected violations of the above and make recommendations to the respective Installation Commander.

f. When in the best interest of the government, the Installation Commander will deny access to any vehicle as deemed appropriate.

3. Hours of Admittance

a. Installation access will normally be granted 24-hours a day. MVs operated by contractors or vendors will only be authorized admittance in conjunction with the operator’s official business aboard MCIEAST Installations.

b. In addition to providing a valid form of identification, individuals may be requested to provide a valid state vehicle registration card, proof of valid state liability insurance, and a valid state driver's license.

c. Sponsors, spouses, or base housing residents may host guests at any hour in accordance with local policy.

d. Visitors may bring their vehicles aboard an MCIEAST Installation for hosted "open to the public" events, but must depart with their vehicles immediately upon completion of the event.

e. Rental cars will be admitted 24-hours a day providing all access control requirements are met for unescorted access and a copy of the rental agreement/contract is provided to the ACP Sentry. An operator without an acceptable credential must first have their identity established, fitness determined, and have an acceptable purpose for entry. If determined qualified for entry, a DBIDS Temporary Pass may be issued.

4. Special Events. The Installation Commander may host special events that are open to the public. When the requirements of this Order or the references cannot be met, compensatory measures will be developed as necessary and appropriate according to the Special Event Vulnerability Assessment for the event. Installation Commanders must request a deviation, an exception, or waiver in accordance with reference (a) when access control requirements cannot be met. Waivers for open base events shall be routed to the Deputy Commandant, Plans, Policies and Operations, Security Division, via the chain of command, a minimum of 120 days prior to the special event.

a. Visitor vehicles are authorized aboard MCIEAST Installations during a special event but must depart immediately upon completion of the event.

b. Unit-level special events require sponsorship from an official representative of the unit.

Chapter 5

Standards for Registration and Passes

1. Vehicle Registration

a. Registration of vehicles is required by active-duty service members, reservists on extended active-duty, reserve service members in the Selected Marine Corps Reserve (SMCR) or Individual Mobilization Augmentation (IMA) Unit, civilian employees, contractors, and privatized housing residents of MCIEAST Installations. Any person that obtains a DBIDS credential to access an MCIEAST Installations are required to register their POV within 30 days of purchase, permanent change of station, or permanent change of assignment, to include other DoD components. Retirees are encouraged to register their vehicles aboard the Installation in which they make the most frequent visits.

(1) The applicant must register their vehicle in person. Spouses may register on behalf of the sponsor. In unusual cases, such as deployment or hospitalization when neither the owner nor the spouse can register in person, a parent, adult family members, a staff noncommissioned officer, officer, or civilian equivalent in the applicant's chain-of-command may represent the owner with an appropriate Power of Attorney (POA).

(2) In all cases, the following documentation is required:

(a) Military, military family member, or civilian ID.

(b) A valid state operator’s license. Temporary or provisional licenses, International Driver’s License, and permits do not satisfy the requirement for registration.

(c) A current state vehicle registration card. Temporary license plates and or temporary registrations do not satisfy the requirement for permanent registration.

(d) Proof of liability insurance meeting the coverage amount requirements established in the laws of the state in which the installation is located.

(e) Proof of completion of the Driver Improvement Course for military members under the age of 26.

(f) If the applicant is not the registered owner, legal owner, or owner’s spouse, a POA is required to register a vehicle. Vehicles belonging to other than immediate family members (i.e., parent, wife, or child) will not normally be registered. However, local policy may allow registering a vehicle that is not owned by the individual, if the vehicle is to be used for an extended period.

(g) Faxes, photocopies, or electronic media are insufficient to prove compliance with state registration requirements; however, they are acceptable to show proof of insurance. In cases involving fleet or lease vehicles, a photocopy may be accepted. Under these circumstances, operators may only be in possession of a photocopy due to the original vehicle registration being maintained by the corporate office.

b. Reserve Service Members. All reserve component service members affiliated with an IMA, SMCR unit, or on orders are authorized to access MCIEAST Installations.

(1) To gain access, a reserve DoD ID must be presented.

(2) For Individual Ready Reserve Marines, a letter from their joining command must list the beginning and end date of the orders.

2. Registration of Motorcycles. Installation Commanders will establish procedures to ensure all motorcycles entering a MCIEAST Installation are properly registered by enforcing the following:

a. Military Personnel

(1) The individual must have signed up for or completed the appropriate, approved motorcycle safety course (MSC).

(2) A service member attempting to enter a MCIEAST Installation on an unregistered motorcycle or without having signed up for or completed an approved course is not authorized to bring the motorcycle aboard the Installation.

(3) Unit Motorcycle Mentorship Program Presidents are responsible for providing their personnel with the procedures for signing up for the appropriate MSC.

(4) The Installation Commander may authorize properly licensed motorcycle operators to ride on their Installation for a brief period, not to exceed 30 days, while the individual is waiting to complete the first available Basic Riders Course (BRC).

(5) Once the BRC is completed and all other required documentation for motorcycle registration is produced, the motorcycle operator may then register the vehicle.

(a) Documentation includes all required documents to register a MV as outlined in paragraph 1a(2) of this chapter;

(b) Current state motorcycle registration card; and

(c) Motorcycle Safety Foundation Course (MSFC) completion card or certificate.

(6) Individuals who fail to complete the MSFC must remove their motorcycle from the Installation immediately.

(7) Motorcycles that are not required to be registered by the State's Division of MVs are exempt from this policy. This includes dirt bikes, mini bikes, ATVs, and mopeds as defined by the state.

b. Civilians, Military Dependents, and Retirees. Although encouraged, civilians, military dependents, and retirees who operate a motorcycle on MCIEAST Installations are not required to attend the MSFC. Documentation required for civilians, military dependents, and retirees to register a motorcycle aboard an MCIEAST Installation includes all required documents to register MV outlined in paragraph 1 and 2a(5) of this chapter, with the exception of the MSFC completion card or certificate.

3. Temporary Passes. DBIDS Temporary Passes (60 days or less) may be issued to accommodate short to intermediate visits or business activities aboard MCIEAST Installations.

a. The DBIDS Temporary Pass will be displayed in the lower left corner of the driver's side windshield. Motorcycle operators will carry the DBIDS Temporary Pass on their person.

b. All DBIDS Temporary Passes will expire at 2359 hours on the expiration date stamped or written on the pass.

c. Consolidated Law Enforcement Operation Center (CLEOC)/Naval Justice Information System (NJIS) database entry will be made by the PMO/MCPD representative to track the individual by the individual's name, company, and the state in which the vehicle is registered.

d. Personnel not affiliated with an organization located aboard the Installation must request authorization in writing to the Installation Commander or their designee to enter the Installation. They must provide an acceptable purpose to visit the Installation, identify a base sponsor, and successfully pass a background check (to establish historic/current fitness) conducted by the PMO/MCPD prior to entry.

4. Special Event Passes. For Special Events, Installation Commanders are encouraged to have guests pre-enroll in DBIDS and obtain a DBIDS Temporary Pass upon arrival to the Installation. However, where this practice is impractical, Installation Commanders may produce a local

Special Event Pass to authorize movement from the point of entry directly to the location of the special event and directly to the designated exit point. Requests for Special Event Passes will be made in accordance with local policy.

5. Restrictions. The privilege of obtaining a DBIDS Temporary Pass is subject to the following restrictions:

a. DBIDS Temporary Passes are government property. The unauthorized removal, sale, transfer to another vehicle, mutilation, forgery, or obscuring of a DBIDS Temporary Pass is prohibited.

b. The registrant must maintain the DBIDS Temporary Pass and safeguard its condition. Loss, mutilation, or defacement of a DBIDS Temporary Pass must be reported to the Installation PMO/MCPD.

c. A registered owner of a MV permanently registered aboard a MCIEAST Installation, or a MV with a DBIDS Temporary Pass, will notify the appropriate VCO or CVO within 24-hours of their transfer from, or termination of, employment. The transfer of title, sale, or significant change of vehicle appearance (e.g., painted a different color) must also be reported. Owners will ensure DBIDS Temporary Passes are removed and returned to the Installation VCO or CVO upon sale of the vehicle.

d. Operators will drive with a valid state operator’s license, valid state registration card, and proof of current state liability insurance in their possession. Motorcycle operators must also carry proof of completion of a MSFC, if required, when riding aboard MCIEAST Installations.

e. Falsifying information contained in an application to permanently register or obtain a DBIDS Temporary Pass may warrant disciplinary action or prosecution.

f. Willful defacement, destruction, or alteration of the manufacturer’s serial or engine number or other distinguishing identification number of a registered vehicle is prohibited and subjects the violator to punitive action.

g. Individuals who operate a MV aboard an Installation must report the suspension or revocation of their driving privileges by any state to Traffic Court and PMO/MCPD within 24-hours of notification of suspension or revocation. Married couples who reside aboard an MCIEAST Installation and who both have had their driving privileges suspended or revoked coordinate removal of their MVs from the Installation until they can be registered in the name of an immediate

family member meeting all qualifications to drive aboard the Installation. Service members living in Bachelor Enlisted Quarters or Bachelor Officer Quarters must remove their vehicle from the Installation until their driving privileges are legally restored.

h. The owner of each vehicle registered on an installation must maintain the minimum insurance required by the state in which the installation is located throughout the period of registration. Failure to maintain adequate and continuous liability insurance coverage may result in a fine by the state, loss of state registration, and loss of Installation driving privileges.

6. Access Passes. To maintain consistency throughout MCIEAST Installations, Installation Commanders will not use any other types or categories of access passes beyond those identified in this Order.

Chapter 6

Standards for Physical Security Access Control

1. Access Control. Access control is designed to restrict and/or control access to an Installation to only those authorized personnel and their conveyances. Installation Commanders will employ access control measures at the perimeter to enhance security and protection of personnel and assets. They may authorize additional security measures based upon the security level, category of individuals requiring access, FPCONs, level of access to be granted, and higher headquarters direction.

2. Minimum Standards for Controlling Physical Access

a. The DoD minimum standards for controlling physical access to an Installation are as follows:

(1) Access may only be granted by utilizing the DBIDS scanner to establish current fitness of all personnel entering MCIEAST Installations in accordance with reference (a), with the exception of paragraph 2.

(2) Compensatory measures will be developed when the requirements of reference (a) cannot be met (e.g., peak traffic, special events, etc.). Note: In accordance with reference (a), if intermittently required due to throughput, traffic, or other circumstances, CACs may be primarily verified visually, with electronic verification performed at random. Non-U.S. citizen CACs (indicated by a blue stripe) must be scanned at ACPs.

(a) When EPACS scanning is not available for access control, security personnel at ACPs will, at a minimum, conduct a physical and visual inspection of cards authorized in reference (a). This inspection includes:

1. Visual match of the photograph on the card to the person presenting the ID.

2. Visual comparison of the card for unique topology and security design requirements.

b. When preparing a local installation access control policy, other considerations for controlling access should include, but are not limited to:

(1) Escort qualifications, responsibilities, and authorizations;

(2) Sponsorship qualifications, responsibilities, and authorizations;

(3) Access privileges at each FPCON;

(4) Mission-essential employee designation, if applicable;

(5) Day and time designation for access;

(6) Locations authorized for access; and

(7) Non-affiliated armed personnel conducting currency escorts.

(8) Appeals process for individuals denied access.

c. MCIEAST Installations will provide reciprocal physical access for CAC and USID issued cardholders. The Installation Commander may limit reciprocal access during increased FPCON levels and emergencies.

d. In the event an individual is debarred from any military installation, access to all MCIEAST Installations will be denied.

3. PPV Housing. For MCIEAST Installations with PPV Housing, the Installation Commander will determine whether to grant Installation access to unaffiliated civilians and their family members for the purpose of occupying PPV housing aboard their Installation. PPV and PMO/MCPD will follow guidance as set forth in reference (g).

a. PPV partners will provide sufficient information to the Installation PMO/MCPD to conduct criminal background checks on all personnel to be assigned PPV housing.

b. PMO/MCPD will provide direction to the PPV partner to determine whether or not the applicants and their family members meet the access control qualifications. The PPV partner has authority to make the final determination on whether to enter into a lease agreement based on these background checks. However, the Installation Commander has authority to make the final determination on who is granted access to their Installation. After a lease is signed, the lessee and family members must bring it to the VCO/CVO for issuing of a DBIDS credential for approved family members.

c. Unaffiliated civilians residing in PPV housing are subject to temporary or permanent debarment in the event of domestic violence, other crimes, or actions deemed inappropriate by the Installation Commander. The Installation PMO/MCPD, in coordination with the Installation Magistrate and SJA, will establish a policy to conduct debarments.

d. In all debarment cases, whether temporary or permanent, the Installation PMO/MCPD must be notified and entries reflecting the debarment must be made in the CLEOC/NJIS and EPACS databases to ensure an unauthorized attempts to re-enter the Installation are unsuccessful.

4. John S. McCain National Defense Authorization Act for FY 2019. MCIEAST Installations will ensure they incorporate unescorted access control procedures in accordance with reference (i), section 621 and section 626.

a. Section 621 grants specific classes of veterans and caregivers certain commissary and Morale, Welfare, and Recreation privileges and contains provisions to extend similar access to surviving spouses, dependent children and other next of kin access to base commissaries, exchanges and other recreational facilities.

b. Section 626 establishes procedures for eligible surviving spouses to obtain unescorted access to installations to receive benefits for which they may be entitled.

5. Photography. In accordance with reference (h), and in the interest of national defense it is unlawful to take, capture, or transmit unauthorized photographs, videos, or images, or render sketches, drawings, maps, or geographical representations of any United States military installation or facility, or do the same of equipment without first obtaining the permission of the Installation Commander. This includes, but is not limited to, dash-mounted cameras, “Go-Pro” style cameras, and similar recording devices.

6. Commercial Vehicle Inspection. Non-governmental commercial vehicles and delivery personnel must undergo a vehicle inspection at the ACP at the respective MCIEAST Installation in accordance with local Commander’s policy. Vehicle inspection site personnel will validate the identity of the driver, bill of lading (if appropriate), and Installation access pass (if required) to ensure all persons meet access control requirements. At a minimum, for the purposes of this Order, a commercial vehicle is defined as any vehicle that meets one or more of the below criteria AND is used for the purpose of commerce:

a. Has three or more axles,

b. A box truck,

c. Any vehicle with a large enclosed storage capacity or capability to transport large quantities of materials (i.e.,: cargo van without windows, trucks with enclosed camper shells, etc.),

d. Is towing an enclosed trailer,

e. Is transporting or designed to transport any hazardous material,

f. Is designed to transport greater than 16 passengers including the driver

Chapter 7

Electronic Physical Access Control System

1. General. DBIDS, the Marine Corps' enterprise EPACS solution, is a DoD owned and operated system developed by the Defense Manpower Data Center as a force protection capability designed to manage personnel, property, and installation access for the DoD. DBIDS is the only EPACS authorized by Marine Corps Installations Command at perimeter ACPs. DBIDS is an access management solutions for vendors, contractors, suppliers, delivery personnel, and all other service providers who require access to Marine Corps Installations on a regularly re-occurring basis. The VCO, CVO, or responsible office will issue these locally produced DBIDS credentials.

2. DBIDS Credentials

a. DBIDS credentials are provided at no cost to individuals who request and meet the requirements to obtain a credential. Vendors, contractors, suppliers, and delivery personnel must apply in accordance with local policy and receive a DBIDS credential if they pass background-screening requirements and are approved by the Installation Commander.

b. DBIDS credential holders who do not drive a "commercial vehicle" may access an MCIEAST Installation via any gate approved by local policy. Commercial vehicles, as defined by local policy, must enter through those gates designated by the Installation Commander, where the vehicles are subject to inspection.

c. All applicants who receive a DBIDS credential are subject to a criminal background check and a vehicle inspection at any time.

3. Access

a. In accordance with reference (a) and chapter 8 of this Order, local first responders and other essential personnel responding to those situations where life and safety require external support from an outside agencies in the performance of official duties are the only exception to the DBIDS enrollment policy; i.e., power company to assist in natural disaster relief.

b. Receiving a DBIDS credential does not constitute approval of proposed business or activities aboard the Installation. Individuals or businesses must appropriately request and receive approval to conduct their proposed business or activity aboard MCIEAST Installations. For example, not-for-profit entities must submit a

written request via the SJA and receive an Installation Commander's specific approval before holding an event aboard the Installation. This request and approval requirement is separate and apart from submitting the appropriate paperwork to gain an access credential.

4. Contractor Access Control Requirements

a. DBIDS credentials are furnished at the Installation VCO or CVO. All lost or stolen badges will be immediately reported to the PMO/MCPD.

b. Contractor/sub-contractor employees must present a letter from the Installation Contracting Officer to the VCO/CVO in order to obtain a DBIDS credential or DBIDS temporary pass. The letter must indicate the relevant contract, contract period, Prime Contractor, expiration date, and days/hours of scheduled work.

c. The Prime Contractor must provide the VCO/CVO a roster of all personnel (to include all sub-contracted employees) who will be employed on the Installation. Prime Contractors are responsible for immediate accountability of all employees in the case of an emergency.

d. The Prime Contractor must provide an updated employee roster (including all sub-contracted employees) to the Installation VCO/CVO within three business days if an employee is terminated for any reason or a new employee is hired. All new hires will complete all Installation access control security procedures prior to performing any work or accessing any MCIEAST Installation.

e. The prime contractor must retrieve all government issued IDs previously issued to a terminated employee and return them to the PMO/MCPD within 24-hours when a contracted employee is terminated for any reason. The prime contractor must immediately notify PMO/MCPD when an employee is terminated for any reason and PMO/MCPD will immediately suspend access for the terminated employee.

f. Prime contractor personnel conducting long-term projects aboard a site may be authorized escort privileges by the installation commander.

(1) Escort guidelines shall be outlined in the official government contract. Escort privileges will be restricted to business purposes (i.e., delivery of material (concrete/asphalt, etc.) and during normal business hours only, unless specifically outlined in the contract terms or authorized by the site commander. Escort privileges granted to contractor personnel shall be limited to non-local, non-reoccurring material deliveries and out of state material deliveries.

(2) Contractors granted escort privileges shall have "Authorized Escort Privileges" indicated on their DBIDS credential. In the absence of EPACS/DBIDS credentials, contractor personnel shall have escort privileges authorized in writing, which must remain with the individual.

(3) All local, reoccurring delivery drivers shall enroll in the local EPACs and be issued a DBIDS credential or temporary pass.

g. For-Hire Drivers, including but not limited to, taxicab, Uber and limousine drivers, are granted access as directed by local policy. All MCIEAST Installation Commanders will require local for-hire companies/drivers to enroll in DBIDS. Only for-hire drivers that are vetted and credentialed in accordance with the references and local policy will be granted access. Vetted for-hire drivers remain subject to random inspections upon entry/exit and while aboard MCIEAST Installations. For-hire drivers that do not have a valid fare with vetted access shall enter an Installation as directed by local policy. Installation Commanders are encouraged to require entry through the Commercial Inspection Site and subject the vehicles to inspection. For-hire drivers operating with a valid fare with vetted access may enter through gates designated by local policy. Non-local for-hire drivers not enrolled in DBIDS may be sponsored by the individual being transported, providing that individual has an appropriate Trusted Traveler identification.

h. Food and product delivery companies shall not be granted access unless the driver has been properly identity proofed and vetted. Justification for vetted delivery drivers' access shall be queried and validated by access control sentries before entry. All delivery vehicles should be inspected, in accordance with local policy, prior to entry and are subject to re-inspection while aboard MCIEAST Installations at the discretion of the Installation Commander. Solicitation by food or product delivery companies is strictly prohibited aboard all MCIEAST Installations.

i. Towing companies shall not be granted access unless the driver has been properly identity proofed and vetted. Justification for entry by a towing company shall be queried and validated by access control sentries before entry. All tow trucks should be inspected, in accordance with local policy prior to entry and are subject to re-inspection while aboard MCIEAST Installations at the discretion of the Installation Commander.

Chapter 8

Standards for First Responder, Local Government, and Essential Personnel

1. First Responder. First responder refers to any law enforcement (LE) and/or security personnel, firefighter, emergency medical technician, and explosive ordnance disposal personnel who provide the initial, immediate response to an all-hazard incident.

2. Local Government. Local government officials are those persons elected or appointed who are visiting an Installation in an official capacity.

3. Essential Personnel. Essential personnel are those individuals needed to ensure the Installation's mission continues and/or those needed to preserve life, and prevent destruction or serious damage to property.

4. Access Control for First Responders, Local Government Officials, and Essential Personnel. Access control for first responders, local government officials, and essential personnel can pose a risk to an Installation if established procedures are not in place and adhered to. In accordance with reference (a), MCIEAST Installation Commanders must establish access control procedures for First Responders in the performance of duties, Local Government Officials on official business, and other essential personnel responding to those situations where life and safety require external support from an outside agency.

a. First Responders

(1) LE. This includes Federal, state and local LE personnel.

(a) On-duty, non-DoD Officers (LEOs), except Federal, not in a requested response to an active incident, shall be granted access and directed to the designated agency for LE investigations and/or warrant issues, or to a designated meeting place for event coordination.

(b) No non-DoD LEOs are authorized access for the purpose of investigations without prior coordination. If approved, the non-DoD LEO shall be escorted by a DoD LE official. Non-DoD LEOs will be authorized to carry their official issued firearms in the performance of their official duties aboard MCIEAST Installations.

(2) Non-DoD first responders responding to a mutual aid request by an MCIEAST Installation Commander shall be granted access after verification has been made by means designated by the respective Installation Commander. Installation security personnel shall expedite the verification process ensuring no delay in mutual aid assistance.

b. Local Government. Local government officials visiting an Installation in an official capacity shall be granted access in accordance with local policy. However, such officials should obtain a DBIDS credential to avoid any potential delays at ACPs.

c. Essential Personnel. Essential personnel shall be granted access in accordance with local policy, in which Installation Commanders must ensure:

(1) Essential personnel are clearly identified in the event of an emergency.

(2) Essential personnel present CAC or other authorized access control credentials to gain access to an Installation during emergencies.

(3) Access by non-essential personnel during an emergency requires authorization by the EOC prior to entry.

Chapter 9

Definitions

Applicant. An individual requesting physical access to a facility and/or Installation.

Biographic Information. Facts of or relating to a person that asserts and/or supports the establishment of their identity. The identity of U.S. citizens is asserted by their social security number and given name. Other biographic information may include, but is not limited to identifying marks such as tattoos, birthmarks, etc.

Escorted Access. A type of access where an individual must be appropriately accompanied at all times to ensure that the escorted individual does not cause unacceptable risk to the safety, security, or efficiency of an installation or its occupants. The escort requirement is mandated for the duration of the individual's visit. Escorted access applies to official government business and is time-constrained by the duration of authorized business that meets requirements for establishing acceptable purpose. Escorted access designation may be provided to persons who have established an acceptable purpose for their presence at the site.

Fitness. A determination based on historic and current information that an individual is likely not a risk to the safety, security, and efficiency of an installation or its occupants.

Identity Proofing. The process of providing or reviewing federally authorized acceptable documentation for authenticity.

Outstanding Warrant. An order for arrest that has not been served. A warrant may be outstanding if the person named is intentionally evading LE, is unaware that an order for arrest has been issued for them, or the agency responsible for execution of the order for arrest has a backlog of warrants to serve, or a combination of these factors.

Physical Access Control. The process of physically controlling personnel and vehicular entry to Installations, facilities, and resources.

Physical Security. That part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, Installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. It is designed for prevention and provides the means to counter threats when preventive measures are ignored or bypassed.

Purpose. An individual's reason for seeking access to an installation.

Reciprocal Physical Access. Mutual recognition of physical access privileges granted by an Installation Commander.

Restricted Area. An area where measures are employed to prevent or minimize incursions and/or interference, and where special security measures are employed to prevent unauthorized entry and/or movement.

Screening. The physical process of reviewing a person's presented biographic and other ID, as appropriate, to determine their authenticity, authorization, and credential verification against a government data source.

Trusted Traveler. Trusted Traveler access allows authorized individuals who have been granted unescorted access, who possess a valid CAC, or a USID, and is over the age of 16, to simultaneously vouch for co-travelers (in the same vehicle or on foot). Trusted Travelers are entirely responsible for the actions of their guests and for meeting all local security requirements.

Unescorted Access. A type of access where an individual is able to travel unaccompanied on an installation but are subject to any controlled or restricted area limitations.

Vetting. An evaluation of an applicant or cardholder's character and conduct for approval, acceptance, or denial for the issuance of an access control credential or physical access.