UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASE
814 RADFORD BOULEVARD SUITE 20302
ALBANY GA 31704-0302

5512.1A
PSD7000
17 Jan 20

MARINE CORPS LOGISTICS BASE ALBANY ORDER 5512.1A

From: Commanding Officer, Marine Corps Logistics Base Albany
To: Distribution List

Subj: INSTALLATION ACCESS CONTROL REGULATIONS

Ref: (a) MCIEAST-MCB CAMPLEJO 5530.15A
(b) DoDM 5200.8 Volume 3, "Physical Security Program: Access to DoD Installations" January 2. 2019
(c) DoD Instruction 1000.13 "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals" December 14, 2017
(d) DoD Instruction 5200.01, Volume 3 "DoD Information Security Program and Protection of Classified Information (SCI)," Ch 1 May 1, 2018
(e) DoD 5400.11-R "Department Of Defense Privacy Program" of Oct 29, 2014
(f) DoD Instruction 5200.08 "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)" Ch 3, November 20, 2015
(g) H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 115th Congress (2017-2018)
(h) MCO 5512.11E
(i) MCO 5580.1D
(j) MCO 5580.2B W/CH 2, December 30, 2015

Encl: (1) Installation Access Control Regulations and Procedural Guidance

1. Situation. Entry onto the installation is a privilege, not a right. Individuals entering the installation must have a bona fide reason for doing so. This includes uniformed military personnel, family members, Department of Defense (DoD) civilian employees, DoD contract employees, and the general public. The Commanding Officer (CO), Marine Corps Logistics Base (MCLB) Albany grants the privilege to gain access to the installation conditionally to those individuals or organizations that meet the minimum qualifications and conform to regulations contained in this Order and references (a) through (j). If someone breaches the terms of this Order, the installation CO may suspend or revoke the privilege. This Order is designed to enhance security and mitigate unauthorized personnel access to the installation.

2. Mission. This Order implements references (a) through (j) and promulgates regulations that address entry, exit, and removal of

individuals from the installation and facilities under the command of the installation CO. It also establishes responsibilities, regulations, and consequences for personnel who, after properly gaining access to the installation, violate this Order.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. All military, civilian, contract, or dependent personnel, and any individual or organization desiring to gain access to MCLB Albany will do so in accordance with the provisions of this Order.

(2) Concept of Operations

(a) The CO conditionally grants the privilege for personnel to gain access to the installation to those individuals or organizations who meet the minimum qualifications and conform to regulations. Personnel will be denied access if they are unable to meet the requirements of this Order identified in Chapter 3, paragraph 2. Removal or denial actions will be reasonable, prudent, and judiciously applied.

(b) To the maximum extent practicable, all individuals granted access to the installation will be subject to a criminal background check as prescribed in references (b), and (i). If determined fit for entry, an Electronic Physical Access Control System (EPACS) credential will be issued. The enterprise solution for EPACS a MCLBA is the Defense Biometrics Identification System (DBIDS).

(c) To the maximum extent practicable, all individuals granted access to the installation will be issued a credential that indicates the identity of the individual, time duration, and any limitations of access granted. This document must remain in the possession of the individual, is not transferable, and must be presented upon demand to any installation security official. All vehicle temporary passes that are issued to individuals will be prominently displayed on the inside of the window or dash of the vehicle.

(d) Nothing in this Order is to be construed as limiting the CO's authority to maintain a secure installation.

b. Subordinate Element Missions. Designated personnel assigned to the Marine Corps Police Department (MCPD) will follow directions as set forth in this Order.

4. Administration and Logistics

a. The Privacy Act System of Records associated with the collection of personally identifiable information is "NM05512-2 Badge and Access Control System Records."

b. Recommendations concerning the contents of this Order may be forwarded to the CO, MCLB Albany via the Director, Public Safety Division. The term "installation" used herein refers to MCLB Albany.

5. Command and Signal

a. Command. This Order is applicable to all military, civilian, family member, contract personnel, and any individual or organization desiring to gain access to MCLB Albany

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

TRIMBLE.ALPHONSO.1076304889 Digitally signed by TRIMBLE.ALPHONSO.1076304889 Date: 2020.01.17 14:34:54 -05'00'

ALPHONSO TRIMBLE

DISTRIBUTION: A

LOCATOR SHEET

Location: _____

(Indicate the location(s) of the copy(ies) of this Order.)

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

Responsibility

1. Visitor Control Center (VCC). The VCC has the primary responsibility for Defense Enrollment Eligibility Reporting System (DEERS)/ Real-Time Automated Personnel Identification System (RAPIDS)/Common Access Card (CAC)/Identification (ID) cards and will comply with reference (h). Specific responsibilities include:

a. CAC. The VCC will issue a CAC to DoD military personnel, DoD civilian personnel, contractors, Appropriated Fund employees, and eligible Non-Appropriated Fund employees who require access to government computerized systems. Both identity proofing and vetting are required to determine the eligibility for access to the installation.

b. ID cards that do not require further identity proofing. The VCC will not require further identity proofing for the following cards because these cards have been identity proofed by the issuing agency.

(1) DoD CAC

(2) Federal Personnel Identity Verification (PIV) credentials.

(3) Non – CAC LRC e.g. credential from local/another ePACS-enabled installation with Identity Matching Engine Security and Analysis (IMESA) functionality.

2. MCPD. The MCPD has the primary responsibility of enforcing the provisions of this Order to include:

a. Ensure only personnel delegated by the Chief of Police perform access control duties to include vetting, authorizing, or denying access.

b. Query authoritative data sources to vet the claimed identity of the individual. The MCPD will also determine fitness by using biographical information. This information may include, but is not limited to: the person’s name, date of birth, and Social Security number.

c. Ensure all visitor(s) are sponsored through VCC. All individuals requesting entry to MCLB Albany will have a valid sponsor, per references (b) and (j).

d. Ensure visitors/non-governmental delivery personnel who have been issued access passes undergo a vehicle inspection at the installation entry control point. Vehicle inspection site personnel will validate the pass to ensure the vehicle operators and all passengers in the vehicle are listed on the pass.

e. Contractors, Vendors and Non-Federal Government Personnel. The VCC will issue appropriate credentials to personnel who require unescorted access to the installation to conduct official government business, but do not require access to government computerized systems. Both identity proofing and vetting are required to determine the eligibility for access to the installation.

f. Card Issuance. The MCPD will refer personnel to the VCC who will issue the appropriate credential in accordance with reference (b).

g. Issue vehicle passes to authorized personnel.

h. Conduct random identity proofing and vetting of persons requiring access to the installation, as determined by the installation CO.

i. The MCPD will not require further vetting for the cards listed in paragraph 1(b) because these personnel have been vetted by the issuing agency. However, eligibility for access to the installation will be verified.

j. The MCPD will develop compensatory measures when the requirements of reference (b), cannot be met (i.e. peak traffic flow periods, special events). This will be coordinated by the installation commander.

k. The MCPD will develop procedures for local first responders' requiring physical access.

l. The MCPD will incorporate the following Trusted Traveler procedure for use during Force Protection Conditions (FPCON) NORMAL, ALPHA, and BRAVO.

(1) The Trusted Traveler procedure allows a uniformed service member or Government employee with a valid CAC, a military retiree with a valid DoD identification credential, or an adult dependent with a valid DoD identification credential to present their identification card for verification while simultaneously vouching for all vehicle occupants.

(2) Trusted travelers are responsible for the actions of all sponsored individuals and for meeting all security requirements for escorts as established by the installation CO.

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

4. Special Events. The CO may approve special events that are open to the public. When the requirements of this Order cannot be met, compensatory measures will be developed as necessary and appropriate.

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

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

5. Mission Assurance (MA). MA will provide vulnerability assessments to MCPD as directed by current directives.

Chapter 2

Identity Proofing, Vetting and Authorized Identification

1. General. DoD CAC is the primary token for access to the installation. Uniformed Services Identification and Privilege (Teslin) cards establishes identity and generally purpose. However, access to the installation is contingent upon authorized privileges.

2. Acceptable Credentials and Identity Source Documents. Applicants will provide a valid and original form of identification from those listed below for the purpose of proofing identity or issuance of a visitor's pass. Prior to acceptance, personnel processing an applicant will screen documents for evidence of tampering, counterfeiting, or other alteration. Documents that appear questionable (e.g., having damaged laminates) or otherwise altered will not be accepted. Altered documents will be held until appropriate authorities are notified, and disposition procedures are authorized. All documents must be 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 Personal Identity Verification (PIV) card. The PIV simultaneously establishes identity and historic fitness.

j. Veteran's Health Identification Card (VHIC). The VHIC simultaneously establishes identity and, if the installation has a medical treatment facility, purpose. The VHIC also establishes purpose for individuals accompanying the cardholder. Any individual accompanying the VHIC holder

must be vetted for determination of fitness and issued a DBIDS temporary pass.

k. Non-federal personal identity verification-interoperable (PIV-I) card. The PIV-I establishes only identity.

l. Transportation Worker Identification Card (TWIC). The TWIC establishes only identity.

m. Federal Personal Identity Verification (PIV) card. The PIV simultaneously establishes identity and historic fitness.

Chapter 3

Physical Security Access Control Standards

1. Access Control. Access control is designed to restrict and/or control access to the installation to only those authorized personnel and their conveyances. The installation CO will employ access control measures at the perimeter to enhance security and protection of personnel, and assets. The installation CO may authorize additional security requirements based upon the security level, category of individuals requiring access, FPCONs, and level of access to be granted.

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

a. Federal PIV and DoD-issued CAC card holders require identity proofing and vetting prior to gaining access to the installation.

(1) Individuals possessing a DoD-issued CAC are vetted to DoD personnel Security standards in paragraphs 2a(1)(a) and 2a(1)(b) of attachment (3) of reference (b) and will be considered identity proofed.

(2) Individuals possessing a DoD-issued card per reference (b) are identity proofed at card issuance sites from Federally authorized installations and will be considered identity proofed.

(3) 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 (b).

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

(5) Vetting and adjudication for individuals receiving government identification credentials as listed in paragraphs 2a(1), (3), and (4) of this Chapter occurs prior to permanent card issuance. Individuals in possession of these identification cards and/or credentials will be considered vetted for unescorted access, per reference (b).

(6) Determination of fitness and vetting for DoD-issued identification and privilege cards (paragraph 2a(2)of this chapter) should not be required for unescorted access, as the issuing office verifies the individual’s direct affiliation with the DoD, or a specific DoD sponsor, and eligibility for DoD benefits and entitlements.

b. Non-Federal Government and non-DoD issued cardholders who request unescorted access must be identity proofed and vetted to determine eligibility for access.

(1) Individuals requesting access will provide justification and/or purpose for access to DoD facilities.

(2) Individuals requesting access that are not in possession of an approved, Government issued card will provide the documents listed in chapter 3, paragraphs 3a through 3m. The documents presented will be reviewed by an authorized security representative for the purposes of identity proofing.

(3) The CO will determine the recurring requirement and frequency for additional checks of non-Federal Government and non-DoD issued card holders based upon local security.

(4) MCPD will query the following government data sources to vet the claimed identity, determine fitness, and deny access, if found to be on the below list, 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) Terrorist Screening Database.

(c) Other sources as determined by the DoD component or installation CO. These can include but are not limited to:

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

2. Department of Homeland Security (U.S. Visit).

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

4. The Foreign Visitor System Confirmation Module (FVS-CM).

(5) Denial of Access. Installation access may be denied if it is determined personnel requesting access are found to be in one of the following categories:

(a) Individual is on the National Terrorist Watch List.

(b) Is not a U.S. Citizen and is illegally present in the U.S. or whose U.S. citizenship, immigration status, or Social Security Number cannot be verified.

(c) Individual is the subject to an outstanding arrest warrant.

(d) Individual has knowingly submitted an employment questionnaire, base access request, or visitor/business pass with false or fraudulent information.

(e) Individual has been issued a debarment order and is currently banned from military installations.

(f) Individual is a registered sexual offender.

(g) Membership within the previous 10 years in any organization that advocated the overthrow of the U.S. Government or affiliated with any active gang;

(h) Is pending any felony charge;

(i) Has been convicted of any felony within the last 10 years

(j) Has ever been convicted of any felony violation, or attempted violation, of the following offenses:

1. Sex crime;

2. Robbery;

3. Arson;

4. Murder;

5. Drugs; or

6. Weapons

(l) Has multiple (three or more) misdemeanor criminal convictions within the previous 10 years.

(k) Any reason the Installation Commander deems reasonable for good order and discipline.

(6) 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.

(7) Appeals Process. In the event that a letter of denial was issued on a contractor/sub-contractor vendor employee, the person whom has been denied has the option of appealing the letter of denial. All appeals must be addressed, in writing, to the MCLB Albany Inspector General within five calendar days from the date on the letter of denial. The contractor/sub-contractor or vendor will submit a letter of appeal to the MCLB Albany Inspector General for the third-tier review. During the third-tier approval review, only the TA/Government Representative can inquire about the status of the appeal. At the conclusion of the third-tier review, the Inspector General will provide to the TA/Government Representative the final decision via correspondence. A final disposition of the appeal will be returned within five business days of receiving the request. Letters may be mailed to or dropped off at the following address:

Commanding Officer (Attn: CIG)
Marine Corps Logistics Base
814 Radford Boulevard Suite 20304
Building 3500, Room 506
Albany, GA 31704-0304

3. Minimum Standards for Controlling Physical Access

a. The DoD minimum standards for controlling physical access to the installation will be:

(1) When Enterprise Physical Access Control Systems (EPACS) are not available for access control, security personnel at access control points, at a minimum, will conduct a physical and visual inspection of cards authorized in reference (b). Police department instructions regarding MCPD Gate procedures cover specific missions to include emergency responders and alarm activations for each gate. Gate inspections include:

(a) Visual match of the photograph on the card to the person presenting the identification.

(b) Visual comparison of the card for unique topology and security design requirements.

(2) When the installation procures an electronic PACS the requirements in reference (b) must be met.

b. Other considerations for controlling access 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.

c. The installation will provide reciprocal physical access to the installation for DoD-issued cardholders authorized by reference (b). The CO may limit reciprocal access during increased FPCON levels and emergencies.

Chapter 4

Visitors

1. General. All personnel entering Marine Corps facilities/installations are screened to ensure access is restricted to authorized persons. Visitors present a different concern and are generally unknown persons who pose an increased threat. Screening and vetting of these persons prior to entry serves to enhance the security posture of the installation.

2. Visitor Screening. All visitors, with the exception of those attending command-sponsored events, will obtain a visitor pass from the VCC (during business hours) or the Main Gate sentry (after business hours). The following credentials are required for issuance of a temporary pass:

a. A valid federal or state government identification containing a photograph.

b. Current/existing state identification and other government issued ID's are both acceptable forms of credentials.

c. If driving a motor vehicle, a valid driver’s license, vehicle registration, and proof of insurance.

d. Sponsors are required to identify names, vehicle information, dates of visit, and purpose, to designated installation personnel when requesting to sponsor an individual(s) aboard the installation. Sponsors are responsible for the conduct of their visitors during their time aboard the installation.

e. Non-governmental delivery personnel requiring access to the installation may be issued a pass not to exceed 30 days. Passes may be renewed at 30-day intervals not to exceed six months. Security personnel shall inspect delivery vehicles at the designated commercial entry control point.

f. To further regulate access control, National Crime Information Center (NCIC) queries shall be conducted of all persons entering the installation, except for command sponsored event attendees. These queries may include driver's license, wants and warrants, and/or criminal history.

3. Sponsorship

a. Active duty/retired personnel and their family members may sponsor guests aboard the installation. Active duty personnel may sponsor contractors (business related) aboard the installation.

b. DoD civilians may sponsor contractors (business related) and guests aboard the installation. Short-term service providers, who require access for less than 72 hours, may be sponsored aboard the installation. Sponsors are required to escort the service provider(s). Service providers requesting unescorted access will be vetted.

c. MCCS employees may sponsor contractors (business related) and guests aboard the installation. MCCS employees may sponsor non-CAC contractor’s family members (spouses and children, if contractor is deployed and only for

the duration of the deployment). In these cases, the family member(s) will need to be vetted.

d. Contractors (permanent party) with CAC access may sponsor contractors (business related) and guests aboard the installation.

e. Only persons issued a CDC name card will be allowed to drop off and pick up children at/from the CDC. Non-affiliated CDC cardholders will be treated as visitors and vetted.

f. Navy Federal Credit Union (NFCU) members who have no other base affiliation will not be allowed to sponsor guests aboard the installation. NFCU members will be allowed access to the credit union only and for the amount of time required to conduct their business upon display of account documentation and obtaining a visitor pass. Base access for non-affiliated NFCU members shall be limited to business banking hours. In addition, historic and/or current fitness inquiries will be conducted on non-MCLB Albany affiliated members.

g. Active Duty/CAC card holders may sponsor off-base deliveries aboard the installation (e.g. food or home goods). Upon producing documentation relevant to the delivery, the Marine Corps Police Department(MCPD) will confirm sponsorship, vet the occupants, and allow access to facilitate the delivery.

h. All Command Sponsored groups or events must be submitted to Base Operations. MCPD will check names against a list if provided by Base Operations. MCPD will ensure that individuals meet the requirements to drive their personally owned vehicles (POV) aboard the installation.

i. All sponsors are responsible for the action of their guests at all times. At no point should a guest be unaccounted for while aboard the installation.

j. All veterans seeking to exercise their privileges in accordance with reference (g) will require an acceptable credential as described in reference (b) and chapter 2, paragraph 2, of this Order, a favorable historic background check, and enrollment in DBIDS. In the event a veteran does not possess a VHIC, the VCC will accept a combination of other acceptable source documents in accordance with reference (b) and local policy, as methods to assist processing veterans for access to the installation.

Appendix A

GLOSSARY

1. Access Control. See "physical access control."

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

3. 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.

4. DoD Issued Card. Cards (other than the DoD CAC) authorized by reference (b).

5. Escorted Individuals. Individuals who require access, without determination of fitness, or who must be accompanied by a sponsor with authorization to escort that individual. The escort requirement is mandated for the duration of the individual's visit.

6. Federal PIV. A physical artifact issued by the Federal Government to an individual that contains a photograph, cryptographic keys, and a digitized fingerprint representation so that the claimed identity of the card holder can be verified by another person (human readable and verifiable) or a computer system readable and verifiable. This card is conformant with the standards prescribed in reference (f).

7. 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.

8. Identity Proofing. The process of providing or reviewing federally authorized acceptable documentation DHS Form I-9 for authenticity.

9. Outstanding Warrant. An outstanding arrest warrant is an arrest warrant that has not been served. A warrant may be outstanding if the person named in the warrant is intentionally evading law enforcement, is unaware that a warrant has been issued for him/her; the agency responsible for executing the warrant has a backlog of warrants to serve, or a combination of these factors.

10. Physical Access Control. The process of physically controlling personnel and vehicular entry to installations, facilities, and resources. Access will be either unescorted or escorted.

11. 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. Designed for prevention and provides the means to counter threats when preventive measures are ignored or bypassed.

12. Reciprocal Physical Access. Mutual recognition of physical access privileges granted by an installation CO.

13. Restricted Access Area. An area where special restrictive measures are employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry and/or movement. Restricted areas are designated and authorized by the installation CO, activity commander and/or director, properly posted, and employ multiple physical security measures.

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

15. Trusted Traveler. A procedure that allows for uniformed service members and spouses, DoD employees, and retired uniformed service members and spouses to vouch for occupants in their immediate vehicle, provided the Trusted Traveler vehicle operator possesses a valid identification card and has a clear NCIC check. Trusted Travelers are entirely responsible for the actions of all occupants in their vehicle and for meeting all local security requirements for escort as established by requirements of the installation CO.

16. Unescorted Individuals. Personnel who have been identity proofed and favorably vetted in accordance with reference (b), are eligible for unescorted access aboard the installation; but are subject to any controlled or restricted area limitations, as appropriate.

17. Vehicle Registration. Contractors, vendors, and students must meet all of the requirements for a temporary pass. Individuals must possess authorized paperwork to be granted access to the installation that indicates the beginning and ending dates of the contract, place, and purpose. The individual's pass will expire on the date that the contract ends. All temporary passes will be stamped with the expiration date of the pass and the (VEH REGS) stamp in red ink only.

18. 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.