DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

MCO 5530.13
PP&O (PS)
7 MAY 2021

MARINE CORPS ORDER 5530.13

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS SITE PERIMETER ACCESS CONTROL

Ref: See Enclosure (1)

Encl: (1) References
(2) Site Perimeter Access Control Policy

Report Required: (1) Monthly Electronic Physical Access Control System (ePACS) Statistics

1. Situation. Access control regulates and/or restricts entrance to Marine Corps sites and is essential to define access privileges and authorities granted by commanders. In accordance with reference (a), Department of Defense (DoD) installations, property, and personnel shall be protected. Access to Marine Corps sites is a privilege extended by the responsible commander in accordance with references (a) and (b). This Order applies to perimeter access only, and does not include additional requirements for access to restricted areas.

2. Cancellation. MARADMIN 533-08, MARADMIN 595-18, MARADMIN 713-19, and MARADMIN 071-20.

3. Mission. In accordance with references (a) through (c), the Marine Corps shall protect personnel, resources, and assets by executing effective access control for Marine Corps sites through uniform policy and procedures which ensure expedited access to authorized personnel while restricting or denying access to persons not meeting conditions and/or requirements for access or who pose a threat to the security and safety of the site.

4. Execution. Commanders shall continuously use all available means and capabilities to determine the fitness of individuals requesting access to Marine Corps installations, depots, training centers, facilities, and off-installation activities on land owned or leased by the Marine Corps, hereafter referred to as "sites." Policies and procedures for establishing purpose, identity, and fitness for access to Marine Corps sites shall be implemented consistently and predictably. Commanders shall publish local concepts of operations, command policies, and tactics, techniques, and procedures consistent with references (a) through (c) and this Order.

a. Conflicting Policies. This Order supersedes any conflicting portion of reference (c) concerning perimeter access control. Conflicting policies and regulations will be reported to the Assistant Deputy Commandant, Plans, Policies and Operations (Security) (ADC PP&O (Security)) for resolution.

b. Mandatory and Advisory Regulations. The requirements of this Order that use the commands "shall," "will," or "must" are mandatory unless specifically deviated, exempted, or waived by the ADC PP&O (Security).

c. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) Marine Corps sites will enable expedited access of authorized United States (U.S.) military, DoD personnel, and military family members.

(b) All persons requesting entry to Marine Corps sites shall have an acceptable purpose to enter; present an approved, valid credential; and be subject to Marine Corps standards and methods to determine identity and fitness of the individual(s) requesting access per reference (b).

(c) Access control determinations are inherently a commander's responsibility. Reference (a) provides commanders the authority to take reasonable, necessary, and lawful measures to maintain law and order to protect personnel and property. Commanders retain discretion and latitude in the application of access control standards to address exigent circumstances, but this authority shall not be exercised in an arbitrary, unpredictable, unreasonable, or discriminatory manner.

(d) Visitors requesting access to Marine Corps sites shall be in possession of an approved DoD or Federal Personal Identity Verification (PIV) Identification (ID) card. Visitors not in possession of an approved DoD or Federal PIV card must present an approved credential as outlined in reference (b) and enclosure (2) of this Order. Driver's license or ID cards presented must meet the minimum standards for the production and issuance of driver's licenses and ID cards issued by states, territories, possessions, and the District of Columbia outlined in reference (d).

(e) In accordance with reference (b), this Order applies to:

1. Grounds of all Marine Corps sites on DoD-owned or DoD-leased land that have a perimeter barrier, such as a fence line or wall; an Access Control Point (ACP); and a method for processing visitors.

2. Sites within the U.S. and its possessions and territories.

3. Sites located in foreign countries if permitted by a standing Host Nation Agreement (HNA), Status of Forces Agreement (SOFA), or other requirements. Commanders shall coordinate access control requirements with Host Nations (HNs) and implement actions necessary to prove the identity, determine the fitness, and validate the purpose for HN partners to access Marine Corps sites to the greatest extent practical, lawful, and permitted by applicable HNA or SOFA.

4. Commanders may extend applicability of this Order to process visitors at sites or grounds of sites under their authority, direction, and control, including sites without a perimeter barrier, ACP/Entry Control Facility (ECF), or other entry control point/method.

(f) This Order does not apply to individual buildings on or off of an installation, space in leased buildings or leased offices, space

managed and operated by federal agencies, contractor facilities, or installations or portions of installations that house non-DoD facilities exclusively. Marine Forces Reserve (MARFORRES) Reserve Training Centers that are owned and operated by MARFORRES exclusively are an exception and shall adhere to policy contained within this Order.

(g) Policies and procedures for establishing purpose, identity, and fitness for access to Marine Corps sites shall be implemented consistently and predictably.

(h) All credential requirements, fitness disqualifications, redress and appeal processes, visitor pass requirements, and a copy of the Privacy Act Statement shall be conspicuously posted at each Visitor Control Center (VCC) and on the site internet homepage.

(i) Access disqualification factors outlined in enclosure (2) shall serve as the primary guidelines for all commanders. Commanders shall address exigent factors not identified in enclosure (2) with the site Staff Judge Advocate (SJA), Provost Marshal (PM)/Police Chief (PC), or other designated site security personnel for further guidance. Unresolved exigent factors shall be directed to ADC PP&O (Security) for guidance.

(j) Deviation authority for temporary relief from perimeter access control requirements is the responsibility of the Commandant of the Marine Corps (CMC). CMC has delegated the authority for temporary relief from perimeter access control requirements to DC PP&O.

(2) Concept of Operations

(a) All persons requesting entry to Marine Corps sites with an ePACS shall be subject to an electronic verification of an approved credential. Approved credentials shall be automatically or manually enrolled in the site ePACS following a Defense Biometric Identification System (DBIDS) scan, after purpose for access to the site has been established. Individuals possessing approved credentials who do not properly enroll are required to obtain enrollment at the site VCC.

(b) All visitors will be directed to the site VCC for processing to verify identity, screening, verification of purpose, and issuance of a proper visitor pass or credential.

(c) Individual access to Marine Corps sites will be conducted at an ACP/ECF designated by the site commander in accordance with references (b) and (c). Commanders may use electronic verification capabilities at docks, piers, and marinas; aerial points of embarkation (APOE); and train stations. At a minimum, commanders shall ensure random antiterrorism measures (RAMs) address the absence of consistent access control at these entry points.

(d) Commanders are not required to use ePACS to support access control decisions where ePACS is inappropriate due to mission, or under limited access control requirements and/or capabilities as defined in reference (b).

(e) Persons requesting access to Marine Corps sites must establish identity by presenting an acceptable and valid credential or providing a combination of source identity documents as outlined in enclosure (2).

(f) All persons requesting access to Marine Corps sites must be vetted by a designated government representative and/or system to:

1. Verify identity.

2. Determine fitness.

3. Verify a purpose for access.

(g) Commanders shall coordinate and expedite access control requirements for local emergency responders in accordance with enclosure (2).

(h) Vehicle decals, window placards, or other signage do not qualify as access credentials, and their use in place of requirements in this Order is prohibited.

(i) Commands requesting waivers to requirements of reference (b) and enclosure (2) for special events, as outlined in paragraph 15c, held aboard Marine Corps sites must include Special Event Planning documentation outlined in reference (e). All waiver requests shall be submitted to the Commander, Marine Corps Installations Command (COMMCICOM), for approval via the chain of command a minimum of 60 business days before the event. Waiver approvals must include a copy to notification to the ADC PP&O, cognizant Marine Forces (MARFOR) Commander, Marine Expeditionary Force (MEF) Commander, and Marine Air Wing (MAW) Commander. Waiver requests will be submitted as outlined in reference (c).

d. Subordinate Element Tasks

(1) Deputy Commandant Plans, Policies and Operations (DC PP&O)

(a) Serve as the service-level office of primary responsibility (OPR) responsible for coordination, development, and execution of physical security policies supporting Marine Corps site access control in accordance with references (a) through (c).

(b) Develop and publish access control policy for Marine Corps sites reflecting requirements outlined in federal law, DoD policy, and Department of the Navy (DON) policy.

(c) Support and participate in the DoD Physical Security Enterprise and Analysis Group (PSEAG) and DoD access control working groups.

(d) Develop and maintain an access control inspection capability, including a Functional Area Checklist (FAC), to support Inspector General of the Marine Corps (IGMC) inspections.

(e) Support and coordinate Total Force access control communication plans with the Communications Directorate (CD).

(f) Ensure access control requirements are promulgated across the Total Force.

(g) Serve as the authority for relief from all access control requirements contained in this Order, via temporary deviations, exceptions, and waivers (DEWs), unless otherwise specified.

(2) Deputy Commandant Installations and Logistics (DC I&L)

(a) Establish, maintain, and sustain a perimeter access control program at Marine Corps sites meeting requirements outlined in this Order.

(b) Direct fielding of ePACS at Marine Corps sites.

(c) Include ACPs, ECFs, and VCCs in master planning to enhance visitor control and management capabilities.

(d) Direct Military Construction (MILCON) funding in support of ACPs, ECFs, and VCCs.

(e) Direct the inclusion of access control capabilities in the Program Objective Memorandum (POM) process to support funding for operations, maintenance, sustainment, and enhancement of ePACS.

(f) Direct inclusion of the Identity Matching Engine for Security and Analysis (IMESA) functionality for site ePACS.

(g) Direct funding for operations, maintenance, and enhancement of IMESA capabilities for site ePACS.

(h) Direct initial approval, maintenance, and sustainment of Information Technology (IT) cybersecurity and Authorization to Operate (ATO) requirements for all ePACS in accordance with reference (f).

(i) Direct the security of Personally Identifiable Information (PII) supporting perimeter access control.

(j) Determine and direct proper personnel staffing of site ACPs/ECFs/VCCs.

(k) Establish and maintain a training program for perimeter security personnel, including ACP, ECF, and VCC personnel, on the requirements, processes, and prohibitions contained in this Order.

(l) Direct required initial and sustainment training for operation of ePACS and access control systems.

(m) Direct proper personnel staffing of site VCCs.

(n) Provide monthly and annual site perimeter access control statistical reporting from Marine Corps sites using ePACS to the ADC PP&O (Security).

(o) Ensure commanders develop and maintain an access control redress and appeal process for individuals denied access to Marine Corps sites.

(p) Ensure all credential requirements, fitness disqualifications, Privacy Act Statements, and redress and appeal processes are conspicuously posted at each VCC and appropriate site internet homepage.

(q) Support access control communication plans with the CD.

(r) Coordinate media information related to access control with site Communication Strategy and Operations (COMMSTRAT).

(3) Deputy Commandant, Combat Development and Integration (DC CD&I)

(a) Direct continued research of access control system requirements and capabilities supporting forward operating sites.

(b) Ensure physical security and access control gaps are included in the Marine Corps Capabilities Gap List.

(4) Deputy Commandant, Manpower and Reserve Affairs (DC M&RA)

(a) Manage and support the official Marine Corps personnel data feeds to Defense Eligibility Enrollment System (DEERS).

(b) Manage and promulgate policy for the Marine Corps operation of the service hosted Real-time Automated Personnel Identification System (RAPIDS).

(c) Manage and promulgate policy for the Marine Corps Uniform Services Identification (USID) Card Program.

(5) Commander, Marine Forces Reserve (COMMARFORRES)

(a) Establish, maintain and sustain a MARFORRES perimeter access control program, meeting requirements outlined in this Order.

(b) Direct fielding and use of ePACS at MARFORRES owned sites.

(c) Include ACPs, ECFs, and/or VCCs in MARFORRES site master planning to enhance visitor control and management procedures and capabilities.

(d) Direct MILCON funding in support of ACPs, ECFs, and/or VCCs for MARFORRES owned sites.

(e) Direct the inclusion of perimeter access control capabilities in the POM process, for MARFORRES owned sites, to support funding for operations, maintenance, sustainment, and enhancement of ePACS.

(f) Direct funding for operations, maintenance, and enhancement of IMESA capabilities for ePACS at Marine Corps Support Facility, New Orleans (MARCORSPTFAC NOLA).

(g) Direct security of PII supporting perimeter access control.

(h) Direct initial approval, maintenance, and sustainment of IT cybersecurity and ATO requirements for ePACS in accordance with reference (f).

(i) Direct required initial and continued training for operation of all access control systems.

(j) Direct monthly and annual access control statistical reporting from sites using ePACS to be provided to ADC PP&O (Security), as

applicable. Site personnel shall obtain access control statistics from DBIDS.

(k) Ensure site commanders of MARFORRES-owned sites develop and maintain a perimeter access control redress and appeal process in accordance with this Order for individuals denied access to MARFORRES owned sites.

(l) Ensure all credential requirements, fitness disqualifications, Privacy Act statements, and redress and appeal processes are conspicuously posted at each site VCC and appropriate site internet homepage.

(m) Direct coordination of access control communications plans with the CD.

(n) Direct MARFORRES COMMSTRAT to coordinate site access control media information with CD.

(6) Deputy Commandant, Information (DC I)

(a) Manage IT systems consistent with DoD IT portfolio management and cybersecurity policies.

(b) Direct the Director, Information Command, Control, Communications and Computers Division (IC4) to support and coordinate perimeter access control IT system security authorities and requirements with affected commanders.

(c) Support reciprocity of Marine Corps ePACS systems IT and cybersecurity requirements with the DoD, other Services, and DoD agencies.

(d) Manage and promulgate policy for the Marine Corps Common Access Card (CAC) Program.

(e) Manage and promulgate policy for the Marine Corps Trusted Associate Sponsorship Program.

(7) Commanders, Marine Forces (COMMARFORs). Commanders of Marine Forces Command (MARFORCOM), Central (MARCENT), Cyber (MARFORCYBER), Europe/Africa (MARFOREUAF), Korea (MARFORK), North (MARFORNORTH), Pacific (MARFORPAC), and South (MARFORSOUTH) will ensure perimeter access control requirements are properly coordinated with the cognizant Geographic Combatant Commander and host site/installation commanders as required.

(8) Inspector General of the Marine Corps (IGMC)

(a) Coordinate with, and support the ADC PP&O (Security) efforts to integrate access control requirements in the 5530 Physical Security FAC.

(b) Coordinate with the ADC PP&O (Security) for subject matter expertise to conduct the 5530 Physical Security FAC as part of the IGMC Inspections Program.

(c) Ensure the 5530 Physical Security Functional Area Checklist (FAC) is included in the IGMC Inspections Program and is designated as Critical or Required Evaluation Function Area.

(9) Director of Communication, Communication Directorate (CD)

(a) Support development and dissemination of access control communication plans for the Total Force.

(b) Support dissemination of access control public announcements for the Total Force.

(10) Site Commanders

(a) Site commanders will establish and maintain a site perimeter access control program that encompasses requirements of this Order.

(b) Site commanders will appoint a site access control officer in writing and provide sufficient resources, staff assistance and authority to implement, manage, and execute an effective perimeter access control program. The access control officer is responsible for coordinating site access control requirements with the PM/PC.

(c) Site commanders will designate the PM/PC, in writing, as the responsible officer for operation of the site ePACS.

5. Administration and Logistics

a. Access Control Forms. The Secretary of the Navy (SECNAV) Form 5512/1, *Department of the Navy Local Population ID Card/Base Access Pass Registration*, shall be used to control perimeter physical access to all Marine Corps sites. Use of any locally produced versions or any other forms to collect and/or maintain PII for the purpose of site access control is strictly prohibited.

b. Privacy Act. Any misuse or unauthorized disclosure of PII may result in both civil and criminal penalties. The Department of the Navy (DON) recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a) and implemented per SECNAVINST 5211.5F.

c. All ePACS will meet Information Assurance requirements outlined in reference (f) and applicable DoD IT and cybersecurity policy.

d. Release of Access Control Records/Information. Access control records and information shall only be released outside of the responsible organization in accordance references (g) through (k).

e. Records Management. Records created as a result of this directive shall be managed according to National Archives and Records Administration (NARA)-approved dispositions per SECNAV M-5210.1 CH-1 to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium. Records disposition schedules are located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-

Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to MCO 5210.11F for Marine Corps records management policy and procedures.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force.

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

G. W. SMITH, Jr
Deputy Commandant
Plans, Policies and Operations

Distribution: PCN 10255301300

REFERENCES

(a) DoDI 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board", with Change 3, dtd 20 Nov 2015
(b) DoDM 5200.08 Vol 3 "Physical Security Program: Access to DoD Installations" with Change 1, dtd 18 Sep 2020
(c) MCO 5530.14A
(d) REAL ID ACT OF 2005
(e) MCO 3302.1F
(f) DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" with Change 3, dtd 29 Dec 2020
(g) DoDI 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities" with Change 1, dtd 29 Nov 2016
(h) 5 U.S.C. Code Section 552a
(i) DoDI 5400.11, "DoD Privacy and Civil Liberties Programs" with Change 1, dtd 8 Dec 2020
(j) DoDD 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense", dtd 7 Jan 1980
(k) SECNAVINST 5211.5F
dtd 20 May 2019
(l) DODM 1000.13, Vol 1 "DoD Identification (ID) Cards: ID Card Life Cycle" with Change 1,dtd 5 Aug 2020
(m) 50 U.S. Code Section 797
(n) Directive-type Memorandum (DTM) 19-012, "Expansion of Patronage for Certain Veterans and Certain Caregivers for Veterans", dtd 30 Dec 2019
(o) Under Secretary of Defense Personnel and Readiness Memorandum "Temporary Credentials for Certain Veterans Ineligible for a Veterans Health Identification Card to Access Commissary, Exchange, and Authorized Morale, Welfare, and Recreation Facilities", dtd 3 Jan 2020
(p) Under Secretary of Defense Intelligence and Security Memorandum "Clarifying Guidance on Installation "Credentials", dtd 8 Apr, 2020
(q) MCO 3040.4

Marine Corps Site Perimeter Access Control

Table of Contents

Marine Corps Site Perimeter Access Control

1. General. Physical access to a Marine Corps site is a privilege extended by the site commander. Access control measures implemented by the commander ensure only authorized DoD personnel or personnel approved by the commander are granted access. Access control is an integral and interoperable capability of physical security. This Order supplements reference (c) with updated perimeter access control requirements outlined in reference (b). All site perimeter access control will be conducted consistent with reference (b).

a. Access control measures standardize personal identification and authentication to DoD installations and facilities including Marine Corps sites and support interoperability with other Federal entities utilizing DoD CAC as the primary authority of individual authenticity, consistent with applicable law.

b. Access control measures shall be tailored to local conditions to support mission accomplishment, enable base defense, safeguard personnel, and protect site facilities and capabilities.

c. Access control provides the commander a means to enforce the removal of, or deny access to, persons who pose a security risk or threaten the safety of the site.

d. Site Commanders will ensure access control policies are posted at the VCC and appropriate site internet homepage.

e. All visitors shall be directed to the VCC for registration and proof of identity, background screening, and determination of purpose or sponsorship. Site commanders shall ensure local policies address maintaining a capability for after-hours visitor control and registration.

2. Site Designation. For the purpose of perimeter access control to Marine Corps sites, all sites will be designated as one of the following:

a. ePACS-enabled with IMESA functionality.

b. ePACS-enabled without IMESA functionality.

c. Non-ePACS-enabled.

3. Purpose for Access. All persons requesting access to a Marine Corps site must have an acceptable and validated purpose, as defined by this policy and the site commander’s guidance. Purpose for authorized access may be established by the presentation of an approved credential in accordance with paragraph 11 and the site commander’s guidance. Purpose may also be established using supporting documentation such as bills of lading, freight bills, Carrier/Distribution Management Office (DMO) Shipment Pickup and Delivery Sheet for Arms, Ammunition and Explosives (AA&E) and other sensitive material. Guest lists for special events (e.g., weddings, command functions/ ceremonies, baby showers, etc.) must be coordinated and approved in writing by the site commander or designated representative. Supporting documentation may be hardcopy or electronic.

a. Purposes acceptable for access and restricted access to a site:

(1) Shall be based on the specific characteristics of each site, and

(2) Shall limit access of visitors:

(a) Through restricted access after normal working hours, based on contract language or personal sponsor.

(b) Through restricted access during weekends or holidays, based on contract language or personal sponsor.

(c) Through designation of a specific ACP through which access is granted for specialized groups (visitor and commercial ACPs).

(d) During Force Protection Conditions (FPCONs) CHARLIE and DELTA. Mission essential personnel shall be designated in writing by the site commander with a copy provided to the site Provost Marshal's Office (PMO)/Marine Corps Police Department (MCPD) or other designated site security personnel. Site commanders are responsible for maintaining accurate rosters of mission essential personnel.

(e) During Health Protection Conditions (HPCONs) CHARLIE and DELTA. Mission essential personnel shall be designated in writing by the site commander with a copy provided to the site PMO/MCPD or other designated site security personnel. Site commanders are responsible for maintaining accurate rosters of mission essential personnel.

(f) Individual's designation as a site emergency responder.

(g) Site commanders will ensure site/local policy addresses ingress/egress permissions for residents living aboard the site during increased FPCONS and HPCONS.

b. Guidance for special events such as Marine Corps Recruit Depot Graduations, Air Shows, Friendship Days, and Independence Day celebration are outlined in paragraph 15.

c. Access for non-mission essential personnel shall be prohibited during FPCONs and HPCONs CHARLIE and DELTA. Mission essential personnel will be designated in writing and the information will be provided to the PM/PC for granting site access.

4. Access Designation. There are three types of access to Marine Corps sites. Persons accessing Marine Corps sites shall be designated as unescorted, Trusted Traveler, or escorted.

5. Unescorted Access. Unescorted designation applies to persons who have properly established their identity and been identity proofed, received a favorable fitness determination, have established an acceptable purpose for access and presence on the site, have a valid requirement for recurring access, and are in possession of an approved DoD or Federal PIV ID card. Commanders are further authorized to approve unescorted access to designated visitors in possession of an approved, valid credential in accordance with guidelines contained in this Order.

a. Commanders may authorize individual recurring, unescorted access under the following conditions:

(1) At ePACS-enabled sites with IMESA functionality: for individuals currently enrolled in a DoD component ePACS with IMESA.

(2) At ePACS-enabled sites without IMESA functionality: for individuals currently enrolled in the local Marine Corps site ePACS.

(3) At non-ePACS-enabled sites: for individuals presenting a CAC, DoD USID card, or Local or Regional DoD Credential (LRC) valid for that particular site.

b. Establishing identity for unescorted access shall be completed by presenting one acceptable and valid credential or by presenting an acceptable combination of source identity documents as identified in Table 1 on page 21 of this Order. Acceptable and valid credentials and source identity documents must:

(1) Be original and current (unexpired).

(2) Not contain the markings "Not Valid for Federal Purposes," "Not For Use as Federal Identification," "Federal Limits May Apply," or any other similar phrase.

(3) In the case of a driver's license or non-driver's identification card issued by a state, territory, possession, or the District of Columbia, be compliant with reference (d).

c. Individuals possessing more than one acceptable and valid credential must use the credential accurately depicting the specific reason/capacity for visiting the site, in accordance with references (b) and (l).

d. Site commanders may not require more than one acceptable and valid credential to establish identity as a standard access control procedure. However, an intermittent requirement to present additional credentials is acceptable as a RAM.

e. Establishing current fitness. Current fitness is established on a recurring and continuing basis only through a review (either on-the-spot at the VCC or daily through the IMESA) of an individual's information through an authorized check of authoritative government sources by authorized personnel (real-time or most recent file from such source). The review shall include:

(1) Terrorism lists, such as the National Crime Information Center (NCIC) Known and Appropriately Suspected Terrorist (KST) file and the Terrorism Screening Database (TSDB).

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

(3) DoD, Services, federal and site-specific debarment lists.

(4) Department of the Navy's criminal justice information system of record.

(5) Other relevant government databases that may be available including:

(a) Other NCIC files, including the National Sex Offender Registry (NSOR).

(b) Criminal justice or immigration databases.

(c) Other government biometric or biographic databases.

f. Commanders may grant short-term (seven days or less) unescorted access to individuals who meet the requirements outlined in this section but do not meet the requirements for recurring unescorted access as described in paragraph 5 if such individuals successfully complete the Visitor Control Process described in paragraph 9.

g. Commanders shall process individuals who meet the requirements for recurring unescorted access as described in paragraph 5 through the perimeter Visitor Control Process at the ACP/ECF in accordance with paragraph 9.

h. Process individuals who do not meet the requirements for recurring unescorted access as described in paragraphs 4 and 5:

(1) Automatic enrollment in accordance with paragraph 12, if eligible; or

(2) The Visitor Control Process at the VCC in accordance with paragraph 9 of this issuance.

i. Granting unescorted access to the following individuals is prohibited:

(1) An individual listed on any U.S. Government terrorism watch list, except as provided for in law, executive order, or DoD policy to further counterintelligence (CI) or counterterrorism (CT) purposes.

(2) An individual with a felony want or warrant.

j. Following coordination with the SJA, PM/PC, and/or designated site security personnel, site commanders may grant unescorted access to a convicted felon in accordance with applicable Federal, state, and local laws after considering appropriate mitigating factors such as the nature and seriousness of the offense, the circumstances surrounding the offense, recency and frequency of the offense, and the individual’s age and maturity at the time of the offense. This discretion does not extend to persons identified under debarment criteria in paragraph 14.

k. Site commanders must conspicuously post the adjudication criteria and redress and appeal process at the site VCC and site internet homepage for those negatively adjudicated.

l. Establishing historic fitness. Historic fitness is established at a specific point in time only by means of a review of the individual’s prior criminal history through a check of the NCIC, the NCIC Interstate Identification Index (also known as “NCIC Triple I”), relevant government databases, and the DON criminal justice information system of record. The

requirement to establish historic fitness for unescorted access may be met by either:

(1) On-the-spot review and adjudication conducted by government personnel at a site or at a centralized processing location.

(2) Previously established historic fitness by any one of the following:

(a) An acceptable, valid credential used to establish identity in accordance with Paragraph 11 and Table 1;

(b) A previously conducted review and adjudication at a site if followed, immediately and without lapse, by enrollment in an IMESA based ePACS for continuous vetting;

(c) The Defense Counterintelligence and Security Agency (DCSA), or predecessor organization, determination that the individual eligible for access to classified information, as long as that eligibility remains in scope; or

(d) A favorably adjudicated Tier 1 or higher background investigation performed by the DCSA or other Federal agency that remains in scope.

m. Citizenship. Unescorted access may be granted to individuals without U.S. citizenship based on the site's characteristics or mission. However, access to non U.S. citizens may be restricted based on the site mission. Acceptable proof of U.S. citizenship can be demonstrated with any one of the following:

(1) An unexpired U.S. passport or passport card.

(2) An original or certified true copy of a birth certificate issued by a U.S. state, territory, possession, or the District of Columbia bearing a raised seal.

(3) A certificate of naturalization (Form N-550 or N-570).

(4) A Consular Record of Birth Abroad.

n. An individual with dual U.S. citizenship will be treated the same as an individual with only U.S. citizenship.

o. Exceptions to unescorted access for Marine Corps sites:

(1) Special events as identified in paragraph 15; and

(2) Emergencies, as identified in paragraph 16; and

(3) Portions of sites consisting of large unoccupied, undeveloped space aboard Marine Corps sites, outside of inhabited areas, or outside of a fence line, if access to such areas does not create unacceptable risk to missions, assets, and personnel;

(4) Sites, or portions thereof, with a mission that requires access to the public; and

(5) A minor under the age of 18 who does not possess an acceptable and valid credential and is accompanied by a parent or guardian who is age 18 or older and has been granted unescorted access.

6. Trusted Traveler. The Trusted Traveler program allows authorized individuals who have been granted unescorted access to vouch for co-travelers in the same vehicle or on foot and enable those co-travelers to obtain site access. Trusted Traveler designation shall only be authorized for persons granted continued unescorted access who have been identity proofed, received a favorable fitness determination, have a valid purpose for access and presence on the site, have a valid requirement for recurring access, and possess an approved DoD or Federal PIV ID card. (NOTE: The DoD Trusted Traveler program is not associated with any other federal agency program.)

a. Trusted Traveler designation allows an individual presenting an approved DoD or Federal PIV ID card installation access and the ability to vouch for accompanying co-travelers who are on foot or are immediate occupants inside a passenger vehicle who are properly seated and secured in accordance with federal, state, and site motor vehicle laws.

(1) The Trusted Traveler designee must have sufficient knowledge of the co-travelers to legitimately vouch for their identity, fitness, and purpose. Co-travelers must present an acceptable and valid credential if identification is requested by Marine Corps Law Enforcement (LE) personnel conducting command authorized RAMs.

(2) The Trusted Traveler designee is responsible for the actions of all co-travelers while they are onsite.

(3) The number of co-travelers may not exceed five individuals per Trusted Traveler unless specifically authorized by the site commander.

(4) Trusted Travelers are responsible for verifying citizenship of co-travelers and are prohibited from vouching for foreign nationals.

b. The Trusted Traveler program may be established at ePACS-enabled sites with or without IMESA functionality.

c. Trusted Traveler programs may not be established at Marine Corps sites without ePACS, with the sole exception of U.S. uniformed military personnel returning to the site in formation. Access procedures for uniformed U.S. military personnel in formation shall be established by the site commander.

d. Individuals without both U.S. citizenship and DoD affiliation are not permitted designation for Trusted Traveler. Foreign nationals shall not be co-travelers and must adhere to requirements in paragraphs 17 (g) through 17 (i) of this Order.

e. The Trusted Traveler program is permitted for site access only during the hours of 0530-2000. The Trusted Traveler program shall be discontinued during the hours of 2000-0530, during which time all occupants of the vehicle are required to present an acceptable and valid credential to PMO/MCPD or other designated site security personnel. Commanders are authorized to suspend Trusted Traveler programs at any time based on local conditions.

f. Trusted Traveler programs are permitted during FPCON NORMAL, ALPHA, and BRAVO. Trusted Traveler programs shall be suspended during FPCON CHARLIE and DELTA. Waiver authority for allowance of the Trusted Traveler program during FPCON CHARLIE and DELTA lies with the Office of the Under Secretary of Defense, Intelligence and Security (OUSD (I&S)), via the Deputy Commandant, Plans, Policies and Operations (DC PP&O), in accordance with reference (b).

g. Trusted Traveler programs are permitted during HPCON ZERO and ALPHA. Commanders should consider suspending the use of Trusted Traveler programs during HPCON BRAVO. Trusted Traveler programs shall be suspended during HPCON CHARLIE and DELTA. Waiver authority for allowance of the Trusted Traveler program during HPCON CHARLIE and DELTA lies with the OUSD (I&S), via DC PP&O, in accordance with reference (b).

h. Trusted Traveler programs shall be suspended in the event of an ePACS failure except:

(1) For uniformed military personnel returning in formation.

(2) For the period of time that a suspension would cause a bona fide traffic safety risk, as determined by the site commander, on a road not owned or managed by the Marine Corps.

(3) When doing so would significantly degrade the site's mission capability as determined by a commander (minimum grade of O-8) at the time of the ePACS failure. This determination requires notification to COMMCICOM, who in turn will notify the ADC PP&O (Security). The ADC PP&O (Security) will notify the DCSA. Such determinations may not be made in advance of an ePACS failure or established generally in policy.

i. When a site's Trusted Traveler program is suspended due to an ePACS failure, co-travelers requesting entry onto Marine Corps sites may be:

(1) Granted unescorted access by presenting an acceptable and valid credential listed in paragraph 11 that establishes identity and meeting requirements to establish fitness and purpose;

(2) Granted escorted access by presenting any acceptable and valid credential as discussed in accordance with paragraph 11; or

(3) Persons who do not possess an approved DoD or Federal PIV ID card will be processed through the Visitor Control Process as a visitor.

7. Escorted Access. Escorted access designation may be provided to persons who have established an acceptable purpose for their presence at the site and is time-constrained by authorized access that meets requirements for establishing an acceptable purpose. Approved escorts must have authorized unescorted site access privileges and must remain with the individual(s) at all times. Individuals unable to meet the identity or fitness requirements for Trusted Traveler or unescorted access may be granted escorted access.

a. Personnel assigned escort duties shall be limited to escorting five visitors. Special event escorted access is outlined in paragraph 15.

b. Escorts shall be provided by the organization or individual responsible for or otherwise associated with the individual's official

government business and must maintain visual contact of the individual(s) they are escorting.

c. Escorts functioning in their personal or official capacity shall be accountable for the conduct of the individual(s) they are escorting in accordance with site security policies and shall report any conduct or malicious actions by an escorted individual that causes a risk to the safety, security, or efficiency of the site or its occupants in accordance with site procedure. Failure to comply with escort duties may result in the temporary or permanent loss of escort privileges.

d. Per reference (b), escorts must be U.S. citizens, have a DoD affiliation, and themselves be granted unescorted access by the site commander, with the exception of those persons identified in paragraph 10b. Contractors in possession of a CAC and providing direct support to a Marine Corps/DoD unit or federal agency may be authorized to escort persons aboard the site for a business purpose. Escort designation and authorization language shall be included in the terms of all contracts.

e. Prime contractor personnel conducting long-term projects aboard a site may be authorized escort privileges by the commander. Escort guidelines shall be outlined in the official government contract. Escort privileges will be restricted to business purposes (e.g., delivery of material such as concrete or asphalt) and during normal business hours only, unless specifically outlined in the contract terms or authorized by the site commander in writing. Escort privileges granted to contractor personnel shall be limited to non-local, non-reoccurring material deliveries and out of state material deliveries. All local reoccurring delivery drivers shall enroll in the local ePACs. Persons shall have escort limits identified on their ePACs credentials after proof of commander’s authorization has been provided. In the absence of ePACs/DBIDS credentials, contractor personnel shall have escort privileges authorized in writing which must remain with the individual.

f. Emergency response personnel responding to an active event aboard a Marine Corps site are excluded from the sponsor requirement. Emergency response access requirements are addressed in paragraph 16 of this Order.

g. Surface Deployment and Distribution Command (SDDC) approved Hazardous Material (HAZMAT) and explosives commercial carriers arriving after hours seeking Safe Haven or Secure Hold will be authorized access to the site in accordance with reference (c), even when the shipment is not consigned to that site.

8. Visitors. Visitors are defined as persons who do not possess an approved DoD or Federal PIV ID card, do not require continued access to the site, and are requesting access to the site for a period not to exceed 60 days. Visitors requiring access longer than 30 days are required to return to the VCC for ePACS registration renewal.

a. All visitors are required to be processed through the Visitor Control Process using the SECNAV 5512/1 Local Population ID Card/Base Access Pass Registration form.

(1) Reference (k) authorizes the DON to obtain PII for vetting purposes prior to granting unescorted site access. The SECNAV 5512/1 will be used as the sole means to collect PII for the purpose of site access control.

(2) Upon successful registration and background check, either a LRC or Base Access Pass will be issued.

(3) All collection, use, maintenance, or dissemination of PII shall be conducted in accordance with the Privacy Act of 1974 as amended and implemented per references (g) through (k).

b. Use of any locally produced or any other forms to collect and/or maintain PII for the purpose of site access control is strictly prohibited.

c. ePACS registrations for visitors shall include access time limitations or explicitly state that visitor access times are unrestricted.

d. Visitors are defined based on the type of the site:

(1) At ePACS-enabled Marine Corps sites with IMESA functionality, a visitor is any individual who is not eligible for automatic enrollment under paragraph 12 as well as:

(a) Not enrolled in IMESA **nor** the local site ePACS; or

(b) Whose enrollment in the local site ePACS has expired.

(2) At ePACS-enabled Marine Corps sites without IMESA functionality, a visitor is any individual who is not eligible for automatic enrollment under paragraph 12 and:

(a) Is not enrolled in the local site ePACS; or

(b) Whose enrollment in the local site ePACS has expired.

(3) At non-ePACS-enabled Marine Corps sites, a visitor is any individual who does not hold a CAC, USID, or LRC issued by the local site or region.

9. Visitor Control Process

a. Visitor Control Process Procedures. Visitors requesting access to Marine Corps sites will be accounted for electronically or manually.

(1) A visitor to a Marine Corps site is required to:

(a) Establish identity using either an acceptable and valid credential or an acceptable and valid combination of source identity documents as described in paragraph 11.

(b) Establish historic fitness, either by performing an on-the-spot background screening or proving historic fitness was previously established.

(c) Establish current fitness.

(d) Establish an acceptable purpose for presence on the site by means of a credential to establish their identity, or;

(e) Establish an acceptable purpose for presence on the site as described in paragraph 3.

(2) During the Visitor Control Process site procedures shall require:

(a) An inspection by VCC employees of all credentials and source identity documents on the front and back for signs of alteration or counterfeit.

(b) Rejection of credentials and source identity documents that appear questionable (e.g., damaged laminates, evidence of tampering) or altered.

(c) Background screening to be conducted by PMO/MCPD or other designated site security personnel.

(d) Confirmation of purpose for access.

(3) Procedures shall require, upon successful completion of the Visitor Control Process:

(a) Visitors with an e-PACS acceptable and valid credential at an ePACS-enabled site, with or without IMESA functionality, to be enrolled in the ePACS.

(b) All other visitors to be issued a pass or credential in accordance with paragraphs 9(b) and 9(c).

(4) The LRC will not be utilized as a privilege card. Privileges related to Army and Air Force Exchange Service (AAFES), Marine Corps Community Services (MCCS), Defense Commissary Agency (DECA), Veterans Services, etc., shall not be added to the card nor will the LRC be utilized to identify any qualifications such as motorcycle safety, emergency services, etc. Only information pertaining to site access will be identified in the remarks portion of the LRC.

b. Short-Term Visitor Passes. Visitors who successfully complete the Visitor Control Process with an acceptable purpose and a duration not greater than seven days, but who are ineligible for enrollment will be issued either:

(1) Short-term personalized paper or plastic pass. The personalized pass shall, at a minimum, identify the visitor's name and the dates for which the pass is valid for access. The pass will be valid for the shorter duration of the visitor's established acceptable purpose or seven days maximum.

(2) Reusable un-personalized pass. Procedures must be in place to enforce the collection of reusable un-personalized passes as visitors exit to prevent reuse. Any such procedures that involve the collection and maintenance of personally identifiable information (to include holding credentials) will be compliant with references (g) and (i).

(3) The Visitor Pass may be electronically produced by the ePACS or hand written, ensuring all required information is identified. Written passes must be maintained in an official logbook.

c. Long-Term Visitor Credentials. The LRC or approved locally issued credential, where DBIDS is not available, may be issued to individuals who do not possess an ePACS-acceptable and valid credential, have successfully completed the Visitor Control Process with an acceptable purpose, have an identified sponsor, and have access permissions with an approved duration longer than seven days. These credentials shall:

(1) Be limited for the duration of the established acceptable purpose, not to exceed 12 months.

(2) Bear the individual's name, photo, issue date, and dates for which the credential is valid.

(3) Be enrolled in the local site ePACS when issued at an ePACS-enabled site with or without IMESA functionality.

(4) Be enrolled in IMESA when issued at an ePACS-enabled DoD site with IMESA functionality.

(5) Not be used to circumvent the Tier 1 background investigation and CAC issuance requirements for individuals eligible for a CAC under Volume 1 of reference (l).

(6) Identify areas/camps authorized for access.

(7) Persons in possession of a DBIDS or LRC, where DBIDS is not available, are not authorized Trusted Traveler or escort privileges.

10. Sponsorship. Sponsors are defined as persons authorized by the site commander to request approval and authorization for persons unaffiliated with the military to access the site.

a. For Marine Corps sites in the U.S. and its possessions and territories, commanders may extend sponsor designation to active and reserve military personnel, military family members above the age of 18, retired military personnel residing on-site, and government civilians who are U.S. citizens.

b. For sites outside of the U.S. and its possessions and territories, in addition to the personnel listed in the paragraph above, commanders may extend sponsor designation to command authorized and vetted HN military, government civilians, and direct support contractors for official business purposes only.

c. Sponsors are authorized to request approval for limited visitor access for social purposes and shall coordinate visitor access with designated site visitor control personnel. Each sponsored person shall complete the VCC process, including a physical credential check, ePACS enrollment, and temporary pass issuance, in accordance with reference (b).

(1) Requests for greater than 50 persons will be treated as a Special Event and addressed as such, in accordance with paragraph 15 of this Order.

(2) Site commanders will publish policy identifying required lead/preparatory time for requests to sponsor persons. This period is intended to provide visitor control personnel proper time to conduct fitness screening and forward the request to the site commander for approval.

d. Sponsorship is limited to non-restricted areas. Visitor access to designated restricted areas or facilities requires the commander's or commander's designated/authorized representative's written approval.

e. Sponsors shall be accountable for the conduct of the individual(s) they are sponsoring in accordance with site security policies. Sponsors shall report any conduct or malicious actions by an escorted individual that causes a risk to the safety, security, or efficiency of the site or its occupants in accordance with site procedure. Failure to comply with escort duties may result in the temporary or permanent loss of sponsor privileges.

f. Support service (e.g., lawn care, cable, power, credit unions, etc.) and vendor (e.g., food, beverage, perishable goods, etc.) contractors are prohibited from sponsoring any person aboard the site, unless previously coordinated with, and approved by the site commander, in writing.

11. Acceptable Source Identity Documents. For the purposes of establishing identity to access a Marine Corps site, persons must be in possession of a valid CAC or provide an acceptable and valid credential in accordance with reference (b) and Table 1 on Page 21.

a. All source identity documents shall be visually inspected for known security features, as applicable, and for signs of alteration or counterfeit. Electronic verification is not required for source identity documents, but is authorized if electronic verification is available. Unless otherwise specified in this section, source identity documents may only be used to verify identity.

(1) Documents must be an original issue and current.

(2) Documents may not be marked "Not Valid for Federal Purposes", "Federal Limits May Apply", or any similar phrase.

(3) Purpose for access must be provided and approved at the time the individual presents an acceptable and valid source identity credential.

(4) Site commanders may not require more than one acceptable and valid credential to establish identity as a standard access control process. However, intermittent requirements to present additional credentials is acceptable as a RAM.

(5) Credentials that appear questionable (e.g., damaged laminates, evidence of tampering) or altered shall not be accepted for any purpose.

b. Credentials Acceptable at non-ePACS-Enabled Sites. Persons assigned access control responsibilities at site without ePACS functionality will accept:

(1) DoD Common Access Card (CAC). Simultaneously establishes identity, historic fitness, and purpose.

(2) Uniformed Service Identification (USID) Card. The DoD USID, also known as the Teslin Card, establishes identity and generally establishes purpose.

(3) Local Registration Card (LRC). Credentials issued by the local site ePACS which simultaneously establish identity, historic fitness, and purpose, as personnel must establish identity and historic fitness, for card issuance. The current Marine Corps LRC is the DBIDS card.

(4) REAL ID-compliant driver's license or identification card. Issued by a state, territory, possession, or the District of Columbia and only establishes identity.

(5) Enhanced driver's license (EDL). Issued by a state, territory, possession, or the District of Columbia and only establishes identity.

(6) U.S. passport or passport card. Issued by the U.S. Government and only establishes identity.

(7) Foreign passport bearing an unexpired immigrant or non-immigrant visa or entry stamp. Issued by foreign governments and only establishes identity.

c. Credentials Acceptable at ePACS-enabled sites without IMESA Functionality. Absent an approved DEW, ePACS-enabled sites without IMESA functionality will accept the credentials listed in paragraph 11(b) of this Order.

d. Credentials Acceptable at ePACS-enabled Marine Corps sites with IMESA Functionality. Absent an approved DEW, ePACS-enabled Marine Corps sites with IMESA functionality will accept:

(1) The credentials listed in paragraph 11(b) of this Order.

(2) LRC issued by another ePACS-enabled Marine Corps site or region with IMESA functionality. These credentials simultaneously establish identity and historic fitness.

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

(4) Veteran's Health Identification Card (VHIC). Persons in possession of a VHIC may be granted unescorted access to sites where eligible benefits exists and are made available to them.

(5) Non-federal Personal Identity Verification-Interoperable (PIV-I). The PIV-I card establishes identity only.

(6) Transportation Worker Identification Card (TWIC). Establishes identity only.

e. Combinations Accepted at all Marine Corps sites. The following combinations of source identity documents shall be accepted at all Marine Corps sites for enrollment purposes:

(1) TWIC used in conjunction with a REAL ID driver's license.

(2) Original or certified true copy of a birth certificate bearing a raised seal, social security card, and REAL ID driver's license. All three documents must bear the same name or a former name as documented on acceptable name change documentation such as a court order, marriage

certificate, or divorce decree. In this situation the birth certificate and social security card are used to establish identity for the purpose of access control.

(3) Table 1 below provides a summary of acceptable, enrollment capable credentials and the associated established requirements.

f. Credentials that fail to scan. A credential that is typically verified and enrolled by scanning that does not properly scan due to defect, destruction, wear, or any other reason may not be used to enroll in the site ePACS or to establish identity or fitness. Commanders may accept a credential that fails to scan as establishing purpose in order to provide one-day unescorted access to an individual who presents another acceptable and valid credential, verified in accordance with Table 1, and are able to establish their identity and fitness. Because the recurring nature of their purpose cannot be validated, commanders may not enroll the individual into the ePACS to facilitate future visits to the installation until such time as a newly issued credential can be verified and enrolled by scanning.

12. Enrollment

a. Eligibility for ePACS Enrollment is:

(1) Available to individuals seeking recurring access who successfully complete the Visitor Control Process and establish their identity by means of an acceptable and valid credential capable of being enrolled in the ePACS as listed in paragraph 11.

(2) Not available to individuals who fail to complete the Visitor Control Process using an acceptable and valid credential or any acceptable combination of source identity documents listed in paragraph 11.

(3) Not available to all individuals at non-ePACS-enabled Marine Corps sites.

(4) Not to be used to circumvent the Tier 1 background investigation and CAC issuance requirements for individuals eligible for a CAC under reference (l).

b. Enrollment of eligible individuals will be accomplished by adding their identity to the local Marine Corps site ePACS and, at ePACS-enabled sites with IMESA functionality, to the IMESA.

TABLE 1. Summary of Acceptable, Enrollment Capable, Credentials and Established Requirements

Acceptable Credential	Non-ePACS enabled sites		ePACS enabled without IMESA site		ePACS enabled with IMESA site		If Acceptable, Establishes:		
	Acceptable	Enrollment Capable	Acceptable	Enrollment Capable	Acceptable	Enrollment Capable	Identity	Historic Fitness	Purpose
CAC	X		X	X	X	X	X	X	X
USID (Teslin)	X		X	X	X	X	X		X[1]
Local or Regional DoD Credential issued by the local site	X		X	X	X	X	X	X	X
Local or Regional DoD Credential issued by another local or regional site					X	X	X	X	
REAL ID-compliant driver's license, enhanced driver's license, or ID card	X		X		X	X	X		
U.S. or Foreign Passport or Passport Card	X		X		X		X		
TWIC					X	X	X		
VHIC					X	X	X		X
Federal PIV					X	X	X	X	
Non-federal PIV-I					X	X	X		

[1] The USID generally establishes purpose, but may not establish purpose at more-restricted Marine Corps sites that do not serve retirees or dependents.

(1) Automatic Enrollment at the ACP. At ePACS-enabled sites with IMESA functionality, in lieu of undergoing the Visitor Control Process at the VCC:

(a) Individuals establishing identity by means of a CAC or USID shall enroll in IMESA and the local Marine Corps site ePACS by presenting their CAC or USID at the ACP.

(b) Individuals establishing identity by means of any other acceptable and valid credential, who have previously enrolled in IMESA at another site, shall be automatically enrolled in the local Marine Corps site ePACS by presenting at the VCC, the same acceptable and valid credential used previously for enrollment in IMESA. However, the site commander may direct purpose be established prior to enrollment.

(2) At ePACS-enabled sites without IMESA functionality, individuals establishing their identity by means of a CAC or USID will be automatically enrolled in the local Marine Corps site ePACS by presenting their CAC or USID at the ACP in lieu of undergoing the Visitor Control Process at the VCC.

(3) Enrollment Validity and Expiration. Enrollment will be valid:

(a) At ePACS-enabled sites with IMESA functionality, for three years from the date of enrollment in IMESA, until the expiration date on the acceptable and valid credential used to establish identity, or until one year without a visit to the site, whichever comes first. Upon the expiration of an individual's credential, the expiration will be propagated to the ePACS at all ePACS-enabled DoD sites with IMESA functionality.

(b) At ePACS-enabled DoD sites without IMESA functionality, for one year from the date of enrollment in the local ePACS, until the expiration on the acceptable and valid credential used to establish identity, or three months without a visit to the site, whichever comes first.

(4) Declined Enrollment. An individual who is eligible to enroll but declines or refuses enrollment, or has declined or refused enrollment in the past, and subsequently returns to the site at a later date shall be processed as a visitor.

c. Enrollment Reciprocity

(1) Site-to-site reciprocity for CAC holders is approved for access to Marine Corps sites. Military members, family members, DoD civilians, and DoD direct support contractors in possession of a CAC shall be registered at the ACP/ECF.

(2) Enrollment conducted at another DoD installation:

(a) Will not be accepted as proof of historic fitness if the enrollment was conducted at an ePACS-enabled site without IMESA functionality.

(b) Will be accepted as proof of historic fitness if the enrollment was conducted at another Marine Corps ePACS-enabled site without IMESA functionality within 30 days.

(c) Will be accepted as proof of historic fitness if the enrollment was conducted at another ePACS-enabled DoD installation with IMESA functionality within 365 days.

13. ePACS Failure Contingencies. Commanders will establish procedures for ePACS-enabled Marine Corps sites with and without IMESA functionality for site perimeter access control during an ePACS failure. Procedures shall include visual and physical inspection of an approved DoD credential or federal privilege ID card at the ACP/ECF; processing of other credential holders through the Visitor Control Process; visual and physical inspection of all credentials; and other applicable procedures to account for the specific characteristics of the site, risk assessments, this Order, and site-level policies.

14. Debarment

a. Background Screening. Persons requesting access to Marine Corps sites shall be subject to a background screening to determine historic and current fitness. Background screening requires applicable personal information to be entered in authoritative government databases. Background screening and fitness criteria shall be conducted by Marine Corps LE or VCC personnel for all visitors.

b. Debarment Criteria. The following criteria applies to all Marine Corps sites. Persons requesting access to Marine Corps sites will be denied access to the site and/or debarred from the site if:

(1) Marine Corps LE or VCC 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.

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

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

(4) The individual has been convicted of crimes encompassing sexual assault or rape.

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

(6) The individual has been convicted of trafficking in persons.

(7) The individual is a registered sex offender.

(8) The individual has been convicted of drug possession with intent to sell or distribute.

(9) The individual has an active arrest warrant from federal, state, local, or other civil LE authorities, regardless of offense or violation.

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

(11) The individual's name appears on any federal or state agency watch list for criminal behavior or terrorist activity.

(12) The individual is debarred entry or access to a Marine Corps site, other DoD installations or facilities, or other federal site or facility.

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

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

(15) 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.

(a) If an individual is identified on the NCIC KST files or TSDB, PMO/MCPD or other designated site security personnel will immediately call the Naval Criminal Investigative Service (NCIS) Multiple Threat Alert Center (MTAC) for further coordination. The MTAC will coordinate with the Department of Justice (DOJ) or FBI and provide handling instructions to PMO/MCPD or other designated site security personnel.

(b) Site access control personnel shall strictly follow the DOJ/FBI engagement protocols as directed by MTAC personnel.

(16) 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.

c. Debarment Orders. Site commanders are required to include debarment criteria, handling instructions, and notification procedures in command policy. All site debarment orders will be coordinated with the SJA office and the PM/PC or other designated site security personnel.

(1) Debarment orders shall be in writing and identify the reasons with details regarding the specific basis for barring access to the site.

(2) The debarment order shall explicitly state the dates for the period of debarment or identify the debarment term as permanent.

(3) Debarment letters shall be hand-delivered. If hand delivery is impractical, debarment letters shall be sent by certified mail to ensure a record of receipt. Site debarment letters shall include the terms of the length of the debarment.

(4) Any oral debarments directed by Marine Corps LE personnel must be approved by the PM/PC or other designated site security personnel. Oral debarments will be coordinated with the site SJA and followed with a written notification within 24 hours or the next business day.

(5) Debarment notifications, including the notification letter and all supporting documents will be maintained by the site SJA and PMO/MCPD or other designated site security personnel.

(6) Site debarment lists shall be maintained by PMO/MCPD or other designated site security personnel. PMO/MCPD or other designated site security personnel shall ensure all debarment information is entered in the Marine Corps or DON criminal justice information system of record.

(a) Site with ePACS shall maintain debarment information on the ePACS at a minimum.

(b) Sites without an ePACS must maintain a written or electronic debarment list at active ACPs/ECFs.

(7) Debarment of a person from one Marine Corps site will be reciprocated at all Marine Corps sites.

(8) The debarment information/list will be used to ensure that unauthorized personnel are not allowed access, and if applicable, charged with trespassing when entry is illegally gained. All debarment lists shall be considered Controlled Unclassified Information (CUI) and marked appropriately. The SJA and PMO/MCPD or other designated site security personnel will review the list on a monthly basis, at a minimum, to ensure the list is current.

d. Debarments Outside of the United States. Commanders shall ensure that actions to debar HN nationals and third country nationals from Marine Corps sites outside the United States and its possessions and territories comply with applicable HNAs/SOFAs or other requirements established between the U.S. and the HN.

e. Appeal for Barred Personnel. The appeals process allows an individual with accurately identified derogatory information that prevents them from establishing historic or current fitness to request an exception due to their specific circumstances, which allows them to be granted unescorted access. Site commanders are required to establish and maintain a command appeal policy that identifies all requirements for barred individuals to request access privileges. The site commander shall be the authority for all debarment actions, to include removal and reinstatement of privileges. Site commanders shall ensure established adjudication criteria and appeal process information is conspicuously posted at the site VCC and site internet homepage.

(1) All appeal requests shall be coordinated with, and staffed through, the SJA and PMO/MCPD or other designated site security personnel. Final determination of all appeal requests will be decided by the site commander. An original commander's written and signed determination will be provided to the individual in person or by registered mail.

(2) Once an appeal has been addressed and an individual has been granted access, the individual will be handled as any other visitor. An individual who completes the Visitor Control Process through appeal will:

(a) Have enrollment designated as completed through appeal in the remarks section of the individual's profile in the ePACS.

(b) Be ineligible for reciprocal acceptance of enrollment and fitness determination at other DoD sites.

(c) Be ineligible for automatic enrollment in the ePACS of other DoD sites in accordance with paragraph 12.

f. Redress for Personnel Denied Access. The redress process allows an individual to de-conflict his or her identity with that of another individual with whom they are frequently or easily mistaken (e.g., two individuals with similar names or identifiers, one with a criminal history and one without), thereby allowing the individual's proper identity to be evaluated for fitness. Redress requires the affected individual to provide additional biographic information (i.e., date of birth, social security number) or biometric information (e.g., fingerprint). Site commanders are required to establish and maintain a command redress policy that identifies all redress requirements for individuals. The site commander is the authority for removal or reinstating debarment actions. Site commanders shall ensure the

established adjudication criteria and redress process is conspicuously posted at the site VCC and site internet homepage.

(1) Any individual who completes the Visitor Control Process and is identified as not suitable for entry to the site will be denied immediate access to the site. Persons denied access shall be provided a copy of the command redress policy.

(2) All redress requests shall be coordinated with, and staffed through, the SJA and PM/PC or other designated site security personnel. Final determination of all redress requests will be signed by the site commander. An original commander's determination will be provided to the individual in person or by registered mail.

(3) Once all redress actions have been addressed and an individual has been granted access, the individual will be handled as any other visitor. An individual who completes the Visitor Control Process through redress will:

(a) Have enrollment designated as completed through redress in the remarks section of the individual's profile in the ePACS.

(b) Be ineligible for reciprocal acceptance of enrollment and fitness determination at other Marine Corps sites.

(c) Be ineligible for automatic enrollment in the ePACS of other Marine Corps sites. Specific sites (e.g., weapons ranges, auxiliary landing fields) may require additional information or documentation to establish an acceptable purpose as these and other site do not serve benefit populations (such as, but not limited to, veterans, retirees and dependents); a DEW request is not required for such policies.

g. Unauthorized Entry. In accordance with reference (m), a property security regulation, or similar order, issued by a commander of a military installation or facility that include parameters for authorized entry to or exit from a military installation, is legally enforceable against all persons, whether or not those persons are subject to the Uniform Code of Military Justice. Military personnel who reenter a site after having been properly ordered not to do so may be apprehended. Civilian violators may be detained and either escorted off the site or turned over to proper civilian authorities. Commanders and PMO/MCPD or other designated site security personnel shall consult with the site SJA office when dealing with any unauthorized entry situations.

15. Special Events. Temporary waivers issued under this paragraph are not considered deviations, and do not require approval of ADC PP&O (Security). Events noted in paragraph 15c require a waiver with approval from COMMCICOM.

a. Marine Corps Recruit Depot (MCRD) Family Days and Graduation Days. MCRD Commanders shall develop Depot Orders and Provost Marshal Instructions (PMIs)/Marine Corps Police Department Instructions (PDIs) that outline access control guidelines for family days and graduations. Orders shall identify requirements for authorized credentials and fitness criteria. Command policy shall require a random percentage of persons entering the Marine Corps site to be subject to background screening and inspection of their vehicles by Marine Corps LE personnel and Military Working Dogs (MWD) for contraband. Commanders are encouraged to designate a primary ingress gate for family and graduation days.

(1) Depot commanders shall ensure policy addresses requirement for limited access control and increased security for restricted areas and critical assets aboard the Depot. Commanders shall further ensure a Special Event Antiterrorism (SEAT) Plan is developed and maintained in accordance with reference (e). The Plan and associated threat assessments shall be subject to updates, as required by changes to the operating environment.

(2) Commanders shall ensure signage is provided for designated traffic routes to and from authorized parking areas.

(3) Commanders shall ensure signage is provided to identify off-limits areas.

(4) Commanders shall ensure access control information is provided to family members prior to arrival for family and graduation days.

(5) Commanders shall coordinate with COMMSTRAT to disseminate appropriate information in response to elevated FPCON/HPCON and comply with additional measures directed by DoD.

b. Officer Candidate School (OCS)/The Basic School (TBS) Family and Graduation Days. OCS/TBS commanders, in coordination with the Commander, Marine Corps Base Quantico, shall develop Marine Corps Base, OCS and TBS orders, and PMIs outlining access control guidelines for family days and graduations. Orders shall identify requirements for authorized credentials and fitness criteria. Command policy shall direct requirements for a random percentage of persons entering the Marine Corps site to be subject to background screening and inspection of their vehicle, by Marine Corps LE personnel and MWD for contraband. Commanders are encouraged to designate a primary ingress gate for family and graduation days.

(1) Commanders shall ensure that policy addresses requirement for limited access control and increased security for restricted areas and critical assets aboard the Marine Corps site. Commanders shall further ensure that a SEAT Plan is developed and maintained in accordance with reference (e). The Plan and associated threat assessments shall be subject to updates as required by changes to the operating environment.

(2) Commanders shall ensure signage is provided for designated traffic routes to and from authorized parking areas.

(3) Commanders shall ensure signage is provided to identify off-limits areas.

(4) Commanders shall ensure access control information is provided to family members prior to arrival for family and graduation days.

(5) Commanders shall coordinate with COMMSTRAT to disseminate appropriate information in response to elevated FPCON/HPCON and comply with additional measures directed by DoD.

c. Open Base Events. Open base events (e.g., Air Shows, Friendship Days, Festivals, holiday celebrations, Open Houses) provide an opportunity for the Marine Corps to host community members and showcase our Marines and military armament. Attendance at an open base event constitutes an acceptable purpose for access to the Marine Corps site. While there is

significant support for open base events, there are also significant risks associated with permitting site access to un-vetted persons. For this reason, all open base events require a waiver to policy outlined in reference (b) and this Order. Waivers for open base events planned to be held aboard Marine Corps installations must be routed to COMMCICOM, via the chain of command, a minimum of 60 days prior to the special event. Waiver approvals will include a Copy to notification to the ADC PP&O (Security), cognizant MARFOR Commander, MEF Commander, and MAW Commander. Waiver requests will be submitted as outlined in reference (c).

(1) The command shall include the following information in the waiver request:

(a) If the special event falls within the below definitions and/or criteria, a SEAT Plan, risk assessment, and threat assessment will be conducted. In addition, commands executing special event planning will produce a SEAT plan and conduct a Special Event Risk Assessment (SERA) in accordance with reference (e). The SEAT Plan shall be developed and maintained for each singular event, including:

1. An announced event, often unique or symbolic, characterized by a large concentration of personnel and/or a personnel gathering where distinguished visitors are involved.

2. An international or domestic event, contest, activity or meeting, which by its very nature, or specific statutory or regulatory authority, may warrant security, safety, or other logistical support.

(b) Security force orders (i.e., Base Order, Battalion/Squadron Order, PMIs/PDIs).

(c) Information concerning the use of MWD, security augmentation forces (SAF), metal detectors, personnel, and vehicle screening areas.

(d) Barrier plans detailing access control points, limited access points, and parking areas, including parking in/around restricted areas.

(e) A statement addressing increased protection or removal of designated assets supporting MARFOR/MEF response capabilities and plans.

(f) The application of RAMs in accordance with reference (e).

(g) Coordination with local LE agencies for traffic control and subsequent turnover and removal of civilians violating federal or state laws.

(2) In addition to the requirements in the waiver request, commanders shall:

(a) Manage increased risk associated with waiving these requirements.

(b) Ensure individuals granted access to the site for the open base event do not have access to areas not associated with the event.

d. Command Ceremonies and Functions. Command ceremonies and functions require coordination and approval by the site commander. Deployment departure/return events and family days do not require special event waivers.

However, commanders shall conduct a SEAT, in accordance with reference (e) for all command ceremonies and deployment departure/return events and ensure effective access control of restricted areas during these events. Security barriers, ACPs, roving patrols, and command personnel will be utilized to maintain visitors in assigned areas/spaces.

e. Marine Corps Community Service (MCCS) Functions. MCCS-sponsored recreational and sporting events open to the general public require all visitors to be subject to the Visitor Control Process. MCCS personnel may provide pre-registration information to Visitor Control Process personnel for advance screening.

(1) During any special event, site commanders with unique mission requirements may establish more restrictive access control requirements.

(2) Additionally, RAMs during the access control process shall include inspection of the vehicle, parcels, and belongings of an individual seeking site access. All access control RAMs and inspections shall be conducted in accordance with the site commander's current, signed policies.

16. Emergency Services Response to Critical Incidents and Emergencies

a. Emergencies and Natural Disasters. In the event that a Marine Corps site is required to request support for an on-site emergency or natural or man-made disaster effort, commanders shall notify the ADC PP&O (Security), via the chain of command.

b. Local Emergency Response Personnel. Local emergency services mutual aid response is critical to supporting emergency incidents aboard Marine Corps sites. Commanders will address access control requirements in local Memorandums of Understanding/Memorandums of Agreement (MOUs/MOAs). Commanders shall ensure emergency access control requirements are outlined in site orders and standard operating procedures.

(1) Commanders will coordinate with local first responder organizations to develop procedures for facilitating access during emergency response events.

(a) Through such procedures, Marine Corps commanders may establish criteria to waive access requirements for first responders to provide mutual aid. The emergency response event constitutes an acceptable purpose for access. Procedures will address local first responder relief from the scene(s) and site egress guidance.

(b) Site ACP/ECF personnel granting access to first responders during an emergency are required to direct local first responders to check in with the site on-scene incident commander to coordinate their activities and prevent mistaken identities that could hinder a coordinated response to the emergency.

(2) Commanders are authorized to require persons accessing a site to present additional credentials during the conduct of RAMs.

(3) MOUs/MOAs shall address access for joint training events.

17. Special Case Access. Unless otherwise indicated, personnel not in possession of an approved DoD credential, Federal PIV ID card, or LRC shall

be subject to the Visitor Control Process per paragraph 9. Unless otherwise indicated in this Order, individuals meeting special case access criteria in sections (a) through (r) below may be authorized unescorted access.

a. Use of Law Enforcement Credentials for Site Access

(1) Federal, state, local, and tribal LE officers/ agents may utilize their credentials for access while conducting active LE operations/investigations and/or responding to emergencies at the site. Examples of LE operations and/or investigations include transporting suspects, witnesses, or victims; transporting evidence and/or contraband; and traveling to their site work center. At Outside of the Continental United States (OCONUS) locations, HN LE personnel are required to coordinate in advance and be escorted by PMO personnel.

(2) ACP/ECF personnel performing access control duties must be familiar with anti-counterfeit and fraud protection measures associated with LE credentials.

(3) Site Marine Corps LE and VCC personnel will physically and visually verify the authenticity of LE credentials used for site access.

(4) When federal LE credentials are presented, (e.g., FBI, U.S. Secret Service, NCIS, Air Force Office of Special Investigation, and U.S. Army Criminal Investigation Division) agents will have unescorted access to the site and escort privileges for personnel and vehicles in all force protection conditions. Federal LE personnel are granted Trusted Traveler/escort privileges with unrestricted escort privileges, in the performance of LE operations, for personnel traveling within their vehicle.

(5) This does not relieve LE officers/agents from conducting appropriate coordination with designated site security personnel or the SJA, nor does it prevent site ACP/ECF personnel from confirming the purpose for access by LE personnel through their respective agencies.

(6) When not in the performance of official duties or capacity shall comply with the requirements of presenting an approved DoD CAC or Federal PIV as outlined in paragraph 11.

b. Certain Veterans and Certain Caregivers for Veterans. In accordance with references (b) and (n), access to DoD sites is authorized for certain veterans and certain caregivers for veterans. The Department of Veteran's Affairs (VA) provides eligible veterans with a VHIC, which is authorized for site access. The VHIC displays the veteran's name, picture, and special eligibility indicators (e.g., Service Connected, Purple Heart, and Former Prisoner of War (POW)) on the front of the card. The VHIC establishes identity and purpose for access. VHIC holders are required to be processed at the Visitor Control Process at Marine Corps site's VCCs to receive unescorted access the site. In some cases, VHIC holders may require a care provider. Care providers, as agreed upon by DoD and the VA, will be issued a letter indicating their role as the primary caregiver or family caregiver.

(1) Veterans and caregivers who visit for the first time are required to enroll in the site ePACS at the VCC.

(2) Sites with DBIDS shall not issue passes or ePACS LRC to veterans who possess a VHIC. Caregivers who possess an acceptable, approved and valid

credential, as outlined in paragraph 11, are required to enroll in the site ePACS at the VCC.

(3) At those sites without an ePACS, a paper pass may be issued.

(4) Veterans and caregivers will only be granted access to those sites where eligible benefits (medical, exchange and Morale, Welfare, and Recreation (MWR) facilities) exist and are made available to them in accordance with reference (n).

(5) Commanders will conduct the Visitor Control Process for all care providers.

(6) Veterans and caregivers are not allowed to sponsor any other person aboard the site, and are not eligible for Trusted Traveler status.

(7) Marine Corps sites in foreign countries shall include language from the HNA/SOFA for authorized use of non-appropriated services by retirees and veterans.

c. Veterans Possessing the Veterans Affairs (VA) Health Eligibility Center (HEC) Form H623A. Some veterans not eligible for the VHIC have been placed in the VA Healthcare Priority Group 8E and issued a HEC Form H623A. In accordance with references (b) and (o), veterans possessing a H623A are authorized access to Marine Corps sites. Veterans requesting access must be in possession of the HEC Form H623A and an acceptable and valid government-issued credential, as outlined in paragraph 11. For access purposes, while the HEC Form H623A establishes purpose and the government approved credential establishes identity, a background screening is required.

(1) Veterans possessing a HEC Form H623A who visit for the first time are required to enroll in DBIDS at the VCC with an acceptable, approved and valid credential, as outlined in paragraph 11.

(2) At those sites without an ePACS, a paper pass may be issued.

(3) Veterans possessing a HEC Form H623A will only be granted access to those sites where eligible benefits (medical, exchange and MWR facilities) exist and are made available to them in accordance with reference (o).

(4) Veterans possessing a HEC Form H623A are not allowed to sponsor any other person aboard the site, and are not eligible for the Trusted Traveler status.

d. Veteran's Identification Card (VIC). Is not approved for access. The VIC alone does not prove identity or support purpose. VIC holders shall be informed that if eligible and want to use their benefits, they are required to contact the VA and obtain a VHIC or HEC.

e. Hunting and Fishing. Non-DoD personnel must be sponsored or have written authorization from the Marine Corps site commander for hunting and fishing privileges aboard the site, including marked waterside areas. Hunting and fishing activities within waterside restricted areas is prohibited. Personnel will be subject to site hunting and fishing regulations as prescribed by the site commander.

f. Non-Government Public Private Venture (PPV) Housing Personnel

(1) Privatized housing residents are considered visitors prior to receiving a LRC/DBIDS card or after the credential has expired. All non-government persons residing in PPV housing are required to be enrolled in an ePACS once the site commander has authorized their approval for PPV housing residency.

(2) Enrollment will be granted for a period of one year. At the end of each year, residents are required to provide proof of authorization for residency and be vetted for fitness.

(3) Project Owner Corporate/Regional Personnel may be issued a LRC/DBIDS card for a period of one year.

(4) PPV Contractors/Subcontractors (sponsored by the Marine Corps site Housing Manager) may be issued a LRC/DBIDS card for one year.

g. Foreign Visitors. Foreign personnel requesting access to a U.S. Marine Corps site to meet with Marine Corps personnel or representatives must be sponsored by a U.S. Service member, civilian or authorized, direct support contractor. Marine Corps sites will adhere to all DoD, DON, Marine Corps and Geographic Combatant Commander policies, and HNAs/SOFAs regarding foreign national visits from specified countries. Foreign personnel requesting access to Marine Corps sites will be identified as accessing the sites for an official or unofficial visit.

(1) Official Visit. An occasion when a foreign national is sponsored by his or her government or by an international organization to perform official business approved by the government.

(2) Unofficial Visit. An occasion when a foreign national who is not sponsored by his or her government or an international organization visits for unofficial purposes or to conduct business which will entail access to information in the public domain. Unofficial foreign visits aboard a Marine Corps sites include attendance to open base community relation events, visits with DoD personnel stationed aboard Marine Corps sites, and other non-official business. OCONUS sites are tasked with developing local policy in compliance with HNAs/SOFAs for foreign national official visits.

h. Foreign National Military Official Visit. Foreign national personnel conducting official visits aboard Marine Corps sites will be assigned a command sponsor for all visits. In all cases, foreign national personnel will be in possession of an Invitational Travel Order (ITO), approved Foreign Visit Request (FVR), or site approved visit authorization to facilitate access to Marine Corps sites. OCONUS sites are tasked with developing local policy in compliance with the HNA/SOFA for foreign national official visits.

(1) Foreign Liaison Officers (FLO). Foreign Liaison Officers (FLOs) are official government representatives from foreign countries that are permitted to work with Marine units. FLOs are under the command of their parent Service. FLOs will be provided ITOs. Each FLO will have an approved extended visit in the Foreign Visits System, a validated purposed document from the hosting Marine Corps command, and have an assigned contract officer appointed in writing.

(2) Personnel Exchange Program (PEP) Officers. Foreign Personnel Exchange Program (PEP) members are military personnel from foreign countries assigned to Marine units. PEPs are assigned to Marine Corps billets and are integrated members of their host units. PEPs do not have authorities to officially represent, obligate, or authorize actions on behalf of the Marine Corps or their parent Service.

(3) International Military Students (IMS). IMS are military personnel from foreign countries assigned to U.S. military training schools or programs. IMS will be issued a DoD-issued USID card in accordance with reference (l).

(4) Access Control Guidelines for Foreign Nationals on Official Business

(a) A DoD ID with a blue stripe establishes only identity and fitness for access control purposes. Individuals in possession of a DoD ID with a blue stripe must establish purpose by means of appropriate documentation, such as ITO, an official letter from their embassy or commander of the foreign military service, and a sponsor letter from the sponsoring Marine Corps command. Individuals will be screened in accordance with reference (b). Additional screening via U.S. Government official databases is authorized.

(b) Individuals in possession of a DoD ID with a blue stripe will only be authorized explicit permissions to access the site(s) to which they are assigned, deemed appropriate for training, or providing necessary support services, such as medical and dental services, exchange and commissary privileges. At ePACs-enabled sites, individuals in possession of a DoD ID with a blue stripe are required to enroll in the ePACS by visiting the VCC and explicit access permissions shall be designated in the site ePACS.

(c) At ePACS-enabled sites with or without IMESA functionality, individuals in possession of a DoD ID with a blue stripe must and shall always be scanned at the site ECF/ACP. Individuals in possession of a DoD ID with a blue stripe will have their ID scanned even during periods when CACs may be primarily verified visually due to throughput, traffic, or other circumstances.

(d) Access to additional Marine Corps sites or other DoD installation requires coordination by the sponsoring command. The sponsoring command will be required to coordinate access to another Marine Corps site or DoD installation with the site commander and the PM/PC and/or Security Officer.

(e) In accordance with references (b) and (p), individuals in possession of a DoD ID with a blue stripe are not allowed to sponsor persons aboard the site or serve as an escort.

(f) In accordance with references (b) and (p), individuals in possession of a DoD ID with a blue stripe are prohibited from participating in the Trusted Traveler program or vouching for co-travelers in their vehicle. All passengers in a vehicle operated by an individual in possession of a DoD ID with a blue stripe are required to be scanned.

i. Foreign National Dependents. As identified in reference (p), foreign national dependents are authorized to accompany a foreign national assigned

to duty with the DoD. Foreign national dependents are referred to as an accompanying family member and are issued the USID or Next Generation (NextGEN) USID card with blue stripe in accordance with reference (l). The NextGEN USID will contain a blue stripe indicating foreign national affiliation.

(1) A USID or NextGen USID with a foreign national affiliation marking establishes only identity for access control purposes. Foreign national dependents in possession of a USID or NextGEN USID with a foreign national affiliation marking must establish purpose by means of appropriate documentation, such as ITO, an official letter from their embassy or commander of the foreign military service, and a sponsor letter from the sponsoring Marine Corps command. The individuals will be screened in accordance with reference (b). Additional screening via U.S. Government official databases is authorized.

(2) All foreign national dependents in possession of a USID or NextGEN USID with a foreign national affiliation marking and whose sponsor is an individual in possession of a DoD ID with a blue stripe, will only be authorized explicit permissions to access the site to which their sponsor is assigned or those providing necessary support services such medical and dental services and commissary and exchange facilities. At ePACs-enabled sites, all foreign national dependents in possession of a USID or NextGEN USID with a foreign national affiliation marking, whose sponsor is in possession of a DoD ID with a blue stripe, are required to enroll in the ePACS by visiting the VCC and explicit access permissions shall be designated in the site ePACS.

(3) At ePACS-enabled installations with or without IMESA functionality, foreign national dependents in possession of a USID, or NextGEN USID with a foreign national affiliation marking must always be scanned at the installation ECF/ACP. Foreign national dependents in possession of a USID, or NextGEN USID, with a foreign national affiliation marking will be scanned even during periods when other types of DoD ID cards, without a blue stripe, may be primarily verified visually due to throughput, traffic, or other circumstances.

(4) In accordance with references (b) and (p), foreign national dependents in possession of a USID or NextGEN USID with a foreign national affiliation marking are not allowed to sponsor persons aboard the site or serve as an escort.

(5) In accordance with references (b) and (p), foreign national dependents in possession of a USID or NextGEN USID with a foreign national affiliation marking, whose sponsor is an individual in possession DoD ID with a blue stripe, are not allowed to participate in the Trusted Traveler program or vouch for co-travelers in their vehicle. All passengers in a vehicle operated by a foreign national dependent in possession of a USID or NextGEN USID with a foreign national affiliation marking, whose sponsor is an individual possessing a DoD ID card with a blue stripe, are required to be scanned.

(6) Access to additional Marine Corps sites or other DoD installation requires coordination by the sponsoring command. The sponsoring command will be required to coordinate access for foreign national dependents in possession of a USID or NextGEN USID to another Marine Corps site or DoD installation with the site commander and the PM/PC and/or Security Officer.

j. Foreign Military Attachés. Foreign Military Attachés and their staffs are accredited diplomats vetted and cleared through the U.S. State Department and assigned to their diplomatic mission.

(1) Foreign military attachés do not receive orders from the DoD, but are officially based in the United States as diplomats. Foreign military attachés who have formally completed the FVR process shall register their U.S.-issued DoD ID cards at those sites where they have established a requirement for valid official business. Any short-notice requests for access inside the 30-day minimum FVR processing window requires the assigned sponsor to coordinate with the country director for site access. Foreign military attachés must meet all requirements for foreign national visitors in paragraph g(2) to obtain access to a Marine Corps site for unofficial visits.

(2) Foreign nationals in possession of DoD ID card shall enroll in the ePACS at each site they visit or are stationed.

(3) If foreign nationals are required to travel to a site where they are not assigned, they shall be required to register in the ePACS prior to entering the site they are visiting. Foreign nationals traveling to sites where they are not assigned shall pre-coordinate registration into the gaining Marine Corps site's ePACS.

(4) Foreign students/visitors on official business will carry approved ITO, FVRs, or other DoD-approved documentation to verify their official business purpose while on any Marine Corps site and will present this documentation to PMO/MCPD or other designated site security personnel.

k. Screening and Vetting. To the maximum extent practicable, all foreign visitors to Marine Corps sites should undergo LE, antiterrorism (AT), and intelligence screening and vetting prior to gaining access. The Marine Corps Intelligence Activity (MCIA) will provide screening and vetting support to Marine Corps sites through the site security manager. In order to facilitate entry:

(1) Official Visits. Site VCC personnel must and shall receive notification and a copy of ITOs or FVRs from the sponsoring unit prior to arrival of foreign nationals and/or their dependents. VCC personnel will confirm with the responsible Foreign Visit Coordinator that the appropriate screening and vetting was completed during the FVR process. The foreign national's sponsoring unit must approve official travel to each Marine Corps site via official orders, and official orders must include restrictions and authorizations for official/unofficial travel.

(2) Unofficial Visits. All foreign nationals, not affiliated with DoD, requesting access for unofficial purposes must initiate the Visitor Control Process at least 96 hours prior to arrival at the Marine Corps site. Site VCC personnel will contact MCIA’s Identity Intelligence 24-hour watch center for LE, AT, and intelligence screening. MCIA will provide the information to the VCC to inform the decision of whether or not to grant access.

(3) Required Information. VCC staff will be provided information listed in 3(a) through (i) for all foreign nationals attempting to gain access to a Marine Corps site, including foreign national visitors who are denied entry for any reason or decide to rescind their request for access.

(a) Name (normally First Name, Middle Name, and Last or Family Name; may also be first four names)

(b) Date of birth

(c) Place of birth

(d) Citizenship

(e) Passport number

(f) Address, including home address, lodging address in the United States, and the person or organization visiting

(g) Point of contact phone number

(h) Meeting location and purpose of visit

(i) Vehicle make, model, and license number

(4) Once foreign nationals are positively identified and screened and the purpose for access has been validated, they shall be issued a visitor pass to allow initial access to the site.

(5) Sponsored foreign nationals eligible for a DoD-approved access credential must register the access credential in the site ePACS within 96 hours. Site commanders shall validate foreign nationals' access credentials via ePACS to confirm the foreign national's access authority.

(6) If a foreign national is reported in an unauthorized absence status, the sponsoring unit will coordinate with PMO/MCPD or other designated site security or VCC personnel to update ePACS profiles for the foreign national and any dependents to alert other DoD sites of this status.

(7) Any security concerns involving credible information that a foreign national or a foreign agent is involved in a criminal incident will be reported to appropriate Marine Corps LE or CI Intelligence personnel.

l. Role Players. Contract Role Players support exercises aboard Marine Corps sites and provide critical training support. All persons designated as an employee or contractor under the Marine Corps Role Player program are subject to requirements contained in this Order as well as any additional requirements outlined in the Marine Corps Role Player Threat Screening Policy.

m. Transportation Worker Identification Credential (TWIC). The TWIC is Department of Transportation approved credential issued by the Transportation Security Administration to maritime workers and commercial motor carriers. The TWIC meets identity proofing requirements. Purpose is established via an electronic or paper bill of lading, the Carrier Appointment System, or signed Transportation Officer delivery/pickup lists.

(1) Drivers visiting a site for the first time are subject to background screening. Once cleared, identification credentials will be registered with the ePACS and simultaneously registered for ongoing

screening. Once enrolled at a site, drivers will proceed directly to the appropriate ECF and have their credentials scanned.

(2) Credentials of drivers returning to the same site will be scanned at the gate, and drivers will be required to establish their purpose for access.

(3) Persons presenting a TWIC are required to show document such as a paper or electronic bill of lading or proof of a coordinated scheduled pickup with the site DMO and the PMO/MCPD as just cause for requiring access to the site.

(4) TWIC access will be authorized during normal working hours established by the site commander. Access is restricted after normal working hours and on weekends and holidays.

(5) In the event an SDDC approved commercial AA&E/HAZMAT carrier seeks emergency support during a critical incident such as a medical emergency, the request for temporary protective status must be approved and coordinated with the site commander.

(6) Deliveries of freight and HAZMAT consigned to the site after normal working hours or on weekends will require coordination by the DMO, the affected unit, and security personnel. Non-DMO, non-official U.S. Government freight such as Federal Express (FedEx®) or United Parcel Service (UPS®) shall be coordinated in accordance with paragraph 17v below.

(7) The receiving command or organization will provide an escort after normal working hours. Escorts must adhere to all requirements in paragraph 7.

n. Surviving Spouse. Surviving spouses and dependents shall be enrolled in ePACS using a USID, if eligible under reference (l), or an acceptable, approved credential in accordance with paragraph 11.

o. Next of Kin/Gold Star. Next of Kin is defined in reference (q) as surviving spouse, blood relatives, adoptive relatives, or a person standing *in loco parentis*. Next of Kin and Gold Star family members meeting criteria for access may request access to a Marine Corps site and be issued a single-day paper pass, LRC card, or be enrolled in the site ePACS with an approved credential identified in paragraph 11.

(1) Gold Star Family members shall be required to complete the Visitor Control Process and enroll in the ePACS before being granted access once a favorable background check is returned and they have met all access requirements.

(2) A command representative will coordinate with the Gold Star Family member and the VCC for an appointment for enrollment purposes.

(3) Gold Star Family members who do not meet the fitness criteria are required to submit an appeal or redress to the site commander, as for any other ePACS applicant.

(4) Once enrolled, Gold Star family members may be provided 24-hours access, except during FPCONs and HPCONs CHARLIE and DELTA.

(5) Gold Star family members are not authorized Trusted Traveler status.

(6) Gold Star family members are not authorized automatic ePACS enrollment to all Marine Corps sites.

(7) Gold Star member access will be granted for one year. The requesting family member shall follow the same procedures to renew access privileges according to this manual.

(8) Marine Corps sites will honor other Service recognition of Next of Kin/Gold Star Family members.

p. Red Cross Volunteers. Red Cross volunteers require a site sponsor and written authorization from the site commander to access the site. Once site authorization has been obtained, Red Cross volunteers shall be subject to the Visitor Control Process and may be issued a LRC for up to one year.

q. DoD Civilian Retirees. The DoD Civilian Retiree Card may be issued to civilians who retire from DoD. The card may not be used for identification purposes. Civilian retirees must provide an approved source identity document and shall be subject to the Visitor Control Process, establish a purpose for site access and/or be sponsored to access the Marine Corps site.

r. MCCS/AAFES Retiree Cards. MCCS and AAFES Retiree Cards may be issued to civilians who retire from MCCS/AAFES. The card is not authorized to be used for identification purposes. Retirees must provide an approved source identity document and shall be subject to the Visitor Control Process, establish a purpose for site access and/or be sponsored to access Marine Corps sites.

s. Federal Personal Identity Verification (PIV) Cards. Non-DoD, Federal PIVs include Homeland Security Presidential Directive-12 (HSPD-12) compliant credentials from the Departments of State, Treasury, Justice, Interior, Agriculture, Commerce, Labor, Health and Human Services, Housing and Urban Development, Transportation, Energy, Education, Veterans Affairs, Homeland Security, and the United States Postal Service.

(1) All persons in possession of a PIV card are considered identity proofed. The PIV establishes historical fitness.

(2) Access may be granted for these persons only when sponsored on site or when their purpose for access has been validated by official orders.

(3) Government persons in possession of a PIV card that cannot provide and/or contact a sponsor or valid purpose will be denied access.

(4) During the enrollment process, persons in possession of a PIV card will have access restricted to normal business hours. PIV cards may not be used for access outside of normal business hours or weekends without the signed approval of the site commander.

t. Federal Personal Identity Verification (Interoperable) (PIV-I) Cards. Non-federal organizations (i.e., commercial organization) supporting the U.S. Government expressed a desire to issue identity cards that are interoperable with federal government PIV systems and trusted by the federal government.

These cards provide a fraud resistant, federally interoperable, and electronically validated identity solution for DoD commercial vendors that interact with the DoD on a recurring basis.

(1) DoD vendors may access with an approved/qualified PIV-I credentials from a provider that has been approved in accordance with the DoD External Interoperability Plan.

(2) A PIV-I access is only authorized in support of a valid and current contract with a Marine Corps site or a tenant organization.

(3) Access to the site requires a copy of the contract to be provided to VCC personnel. All persons assigned to the contract and requiring access must be listed on the contract proper or in an approved, signed appendix to the contract.

(4) PIV-I personnel are required to be processed through a Visitor Control Process.

(5) Enrollment in ePACS is authorized for the contract period up to a maximum of three years.

(6) PIV-I card holders are considered identity proofed; however, access may be granted for these persons only when sponsored on base or when their purpose for access has been validated and confirmed.

(7) Persons in possession of a PIV-I card that cannot provide a sponsor will be denied access to the site.

(8) Required access to the site after normal working hours and on weekends and holidays must be outlined in the contract. If not addressed in the contract, service provider access to the site shall be restricted to normal working hours Monday through Friday, as established by the command. Access after normal working hours and on weekends and holidays shall be restricted.

u. Local Service Providers. Local service providers are persons working with corporations providing direct service support to the site under contractual agreements. Examples of local service providers include soft drink retailers, consumable items retailers, and local/regional vendors requiring continuous access to provide product support to site commands.

(1) Local service providers shall be enrolled in the ePACS at the VCC with proof of contractual obligations with unit(s) aboard the site.

(2) Local service providers shall be enrolled in the ePACs with their REAL ID-compliant driver’s license.

(3) Site access guidelines shall be addressed in the contract.

(4) Site access shall be provided in accordance with contract terms.

(5) Required access to the site after normal working hours and on weekends and holidays must be outlined in the contract. If not addressed in the contract, service provider access to the site shall be restricted to normal working hours Monday through Friday, as established by the command.

Access after normal working hours and on weekends and holidays shall be restricted.

v. Commercial Transportation. Commercial transportation is any service in which a vehicle owner or operator provides transportation for a fee, including taxi services; transportation network companies and ridesharing services; and mass transit such as buses and trains.

(1) Commercial transportation operators are authorized access to Marine Corps sites for commercial transportation business purposes only. The driver's access shall be temporary and limited in scope and time to what is necessary to fill this acceptable purpose.

(2) Commercial transportation operators must meet all requirements for unescorted visitor access in paragraph 5 of this Order, including enrollment in ePACS.

(a) The driver's acceptable purpose is providing transportation to the passenger, including accessing the site to pick up the passenger(s). ACP/ECF personnel shall require taxi, rideshare, and other commercial transportation operators to provide the name of the requesting passenger and location of the pick-up location.

(b) Commercial transportation operators will be sponsored by an approved sponsor in accordance with paragraph 10.

(c) OCONUS sites are tasked with developing local policy in compliance with HNAs/SOFAs for foreign commercial transportation operators.

w. Personal Delivery Operators. Personal delivery operators are authorized access to Marine Corps sites for business delivery purposes only, such as food and parcel delivery. The driver's access shall be temporary and limited in scope and time to what is necessary to fill this acceptable purpose.

(1) Delivery operators must meet all requirements for unescorted visitor access in paragraph 5 of this Order, including enrollment in ePACS.

(2) Commercial transportation operators will be sponsored by an approved sponsor in accordance with paragraph 10.

(3) Site commanders shall designate a responsible office/agency to serve as a primary sponsor for all local service deliveries (e.g., Amazon, UPS, FedEx, etc.).

x. MILCON and Major Renovation Contractors. Contractors supporting MILCONS, building renovation, and other long-term construction activities shall be provided an ePACS credential for access to the site. All contracts shall include language that addresses the Marine Corps and site access control requirements, and access to the site will be provided in accordance with these terms. Access to the site after working hours stipulated in the contract shall require coordination with the site's Facilities or Public Works Office and PMO/MCPD or other designated site security personnel. Day-use LRCs will not be used to circumvent the vetting and screening process.

18. Unmanned Access Control Points (ACPs)

a. Unmanned Pedestrian ACP. At ePACS-enabled sites with IMESA functionality, commanders may implement unmanned (also known as unattended) ACPs for pedestrian use only. Unmanned Pedestrian ACPs with a single on-site attendant servicing multiple lanes are not considered unmanned pedestrian ACPs. Unmanned pedestrian ACPs are subject to the following requirements:

(1) Only an approved DoD credential or Federal PIV ID card that has already been enrolled at the site may be accepted at unmanned ACPs.

(2) Two-factor authentication is required at all times. The second factor shall be either personal identification number or biometric.

(3) The unmanned pedestrian ACP must:

(a) Be covered by surveillance cameras that are recorded and monitored at all times, either manually or by automated means (i.e., motion detection). Recordings will be kept in accordance with Records Schedule 5000-103.

(b) Prevent vehicular access.

(c) Include a mechanism to prevent the entry of more than one person in a single attempt.

(d) Include tamper alarms which are monitored at all times, and maintain a response force capable of reaching the unmanned pedestrian ACP within 15 minutes of alarm.

(e) LRCs from other sites are prohibited to access unmanned pedestrian ACPs.

(f) Be securely locked with a chain and lock, to prevent operations in the event of a failure of cameras, recording systems, or lack of a tamper alarm on gate operations systems.

(g) Be provided security lighting to support surveillance cameras and allow security forces to view pedestrians at the ACP and to points 30 feet in all directions from the ACP.

b. Unmanned Perimeter Vehicle ACP. Unmanned perimeter vehicle ACPs are authorized at Marine Corps sites to support operational requirements only.

(1) Unmanned perimeter vehicle ACPs require notification to the OUSD (I&S) for consideration. Commands requesting relief from policy, must submit a waiver or exception and forward the request, via the chain of command, to ADC PP&O (Security) for consideration for endorsement and coordination with OUSD (I&S).

(2) No unmanned perimeter vehicle ACP is authorized for personal access convenience.

(3) No unmanned perimeter vehicle ACP is authorized for access by dependents.

(4) Operations of unmanned ACPs require:

(a) Access privileges limited to the minimum number of personnel required to support operations.

(b) Access privileges to and through the unmanned perimeter vehicle ACP assigned in writing by the commander.

(c) Operation of and access to the unmanned perimeter vehicle ACP granted only through the use of two factor authentication.

(d) Be covered by surveillance cameras that are recorded and monitored at all times, either manually or by automated means (i.e., motion detection). Recordings will be kept consistent with applicable records schedules and no less than 30 days.

(e) Tamper alarms which are monitored at all times, and maintain a response force capable of reaching the unmanned perimeter vehicle ACP within 15 minutes of alarm.

(f) LRCs from other sites are prohibited to access unmanned perimeter vehicle ACPs.

(g) The perimeter unmanned vehicle ACP to be under visual observation of an armed person, or locked with a chain and lock, to prevent operations, in the event of a failure of cameras, recording systems, or lack of a tamper alarm on gate operations systems.

(h) Be provided security lighting to support surveillance cameras, safe operations of vehicles and allow security forces to view the ACP and vehicle traffic at the ACP to points 30 feet in all directions from the ACP.

Glossary of Acronyms and Abbreviations

For the purpose of this Order, the following acronyms and abbreviations apply:

AA&E	Arms, Ammunition and Explosives
AAFES	Army and Air Force Exchange Service
ACP	Access Control Point
ADC	Assistant Deputy Commandant
APOE	Aerial Point of Embarkation
AT	Antiterrorism
ATO	Authority to Operate
CAC	Common Access Card
CD	Communications Directorate
CD&I	Combat Development and Integration
CI	Counterintelligence
CMC	Commandant of the Marine Corps
COMMCICOM	Commander, Marine Corps Installations Command
COMMSTRAT	Communications Development and Strategy
CT	Counterterrorism
DBIDS	Defense Biometric Identification System
DC	Deputy Commandant
DCSA	Defense Counterintelligence and Security Agency
DECA	Defense Commissary Agency
DEERS	Defense Enrollment Eligibility Reporting System
DEW	Deviation, Exception or Waiver
DMO	Distribution Management Office
DoD	Department of Defense
DOJ	Department of Justice
DON	Department of the Navy
ECF	Entry Control Facility
EDL	Enhanced Driver’s License
ePACS	electronic Physical Access Control System
FAC	Functional Area Checklist
FBI	Federal Bureau of Investigation
FedEx®	Federal Express
FLO	Foreign Liaison Officer
FPCON	Force Protection Condition
FVR	Foreign Visit Request
HAZMAT	Hazardous Material
HEC	Health Eligibility Center
HN	Host Nation
HNA	Host Nation Agreement
HPCON	Health Protection Condition
I	Information
I&S	Intelligence and Security
I&L	Installation and Logistics
IC4	Information, Command, Control and Computers Division
ID	Identification
IGMC	Inspector General Marine Corps
IMESA	Identity Matching Engine for Security and Analysis
IMS	International Military Student
IT	Information Technology
ITO	International Travel Orders
KST	Known or Suspected Terrorist
LE	Law Enforcement
LRC	Local or Regional DoD Credential

MARCORSPTFAC	Marine Corps Support Facility
MARFOR	Marine Forces
MARFORCENT	Marine Forces Central
MARFORCOM	Marine Forces Command
MARFOREUR/AF	Marine Forces Europe and Africa
MARFORK	Marine Forces Korea
MARFORNORTH	Marine Forces North
MAROFORPAC	Marine Forces Pacific
MARFORRES	Marine Forces Reserve
MARFORSOUTH	Marine Forces South
MAW	Marine Air Wing
MCCS	Marine Corps Community Services
MCIA	Marine Corps Intelligence Activity
MCICOM	Marine Corps Installations Command
MCPD	Marine Corps Police Department
MCRD	Marine Corps Recruit Depot
MEF	Marine Expeditionary Force
MILCON	Military Construction
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTAC	Multiple Threat Assessment Center
MWD	Military Working Dog
MWR	Morale Welfare and Recreation
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative
NextGen USID	Next Generation U.S. Identification Card
NOLA	New Orleans Louisiana
NSOR	National Sex Offender Registry
OCONUS	Outside of the Continental United States
OCS	Officer Candidate School
OPR	Office of Primary Responsibility
OUSD	Office of the Under Secretary of Defense
PC	Police Chief
PDI	Police Department Instruction
PEP	Personnel Exchange Program
PII	Personally Identifiable Information
PM	Provost Marshal
PMI	Provost Marshal Instruction
PMO	Provost Marshal’s Office
POM	Program Objective Memorandum
POW	Prisoner of War
PP&O	Plans, Policies and Operations
PPV	Public Private Venture
PS	Plans, Policies and Operations Department, Security Division
PSEAG	Physical Security Enterprise and Analysis Group
RAM	Random Antiterrorism Measure
RAPIDS	Real- Time Automated Personnel Identification System
SAF	Security Auxiliary Force
SDDC	Surface Deployment and Distribution Command
SEAT	Special Event Antiterrorism
SECNAV	Secretary of the Navy
SERA	Special Event Risk Assessment
SOFA	Status of Forces Agreement
SJA	Staff Judge Advocate
TBS	The Basic School
TRIPLE I	Interstate Identification Index

TSDB	Terrorist Screening Database
TWIC	Transportation Worker Identification Credential
UPS®	United Parcel Service
U.S.	United States
USID	United States Identification Card
VA	Veterans Affairs
VCC	Visitor Control Center
VHIC	Veteran Health Identification Card
VIC	Veteran Identification Card

Glossary of Terms and Definitions

For the purpose of this Order, the following terms and definitions apply:

Acceptable Credential. A credential that, depending on the type of installation, must be accepted as proof of identity, historic fitness, or purpose in accordance with Section 5.1 of Ref (b). (DoDM 5200.08 Vol 3)

Access Control Point (ACP). Identified gap in an installation's/site's perimeter security for pedestrian and/or vehicular access. Often called an entry control point or simply "gate". Includes commercial vehicle inspection points. (DoDM 5200.08 Vol 3)

Appeal. A process for an individual with accurately identified derogatory information that prevents individuals from establishing either historic or current fitness to seek an exception due to their specific circumstances, allowing them to be granted unescorted access. (DoDM 5200.08 Vol 3)

Caregiver. Defined in Section 1720G(d) of Title 38, U.S.C.

Credential. A form of identification that, on its own, associates a specific person with their specific identity, biographic, and, in some cases, biometric information. For example, a driver's license. A document that contains identity information but cannot be associated with a specific person (for example, if it has no photograph or biometric information) is not a credential, but may be a source identity document. (DoDM 5200.08 Vol 3)

Current Fitness. A determination that an individual has no pending criminal cases or actions against him or her and is not listed on any U.S. Government terrorism lists that would indicate that such individual may pose a risk to the safety, security, and efficiency of the installation/site or its occupants. (DoDM 5200.08 Vol 3)

Deviation. A divergence from a requirement or procedure that is not intended to be temporary or corrected. (DoDM 5200.08 Vol 3)

Electronically Verify. The process of confirming, by cryptographic means or querying the original issuer, that a presented credential is authentic (not counterfeit) and still valid (not revoked, cancelled, or otherwise reported lost, stolen, or compromised). (DoDM 5200.08 Vol 3)

Electronic Physical Access Control System (ePACS). An information technology system that provides a "grant" or "deny" decision or recommendation based on a presented identification card, optional additional authentication factors such as a PIN or biometric input, an identity database, and one or more business rules that determines which individuals are authorized access. (DoDM 5200.08 Vol 3)

Enrollment. A process that allows individuals who anticipate a subsequent visit to the installation/site to persist their established fitness, but not purpose, facilitating future entry. (DoDM 5200.08 Vol 3)

Enrollment Reciprocity. The acceptance of an enrollment conducted at another DoD installation/site as proof of an individual's established fitness, but not purpose. (DoDM 5200.08 Vol 3)

Escorted Access. Access to which an individual must be accompanied at all times to ensure that the escorted individual does not cause unacceptable risk to the safety, security, or efficiency of an installation/site or its occupants. (DoDM 5200.08 Vol 3)

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/site or its occupants. (DoDM 5200.08 Vol 3)

Historic Fitness. A determination that an individual's criminal history reflects a level of character and personal conduct that does not pose a risk to the safety, security, and efficiency of an installation or its occupants. (DoDM 5200.08 Vol 3)

Installation. The grounds of, but not buildings on, a base, camp, post, station, yard, center, homeport facility for any ship, or other activity under DoD jurisdiction, including any leased facility, that is located within any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, or Guam that have a perimeter barrier (such as a fence line or wall), one or more access control points (sometimes called entry control points), and a method for processing visitors. Such term does not include any facility used primarily for civil works, rivers and harbors projects, or flood control projects. (DoDM 5200.08 Vol 3)

Purpose. An individual's reason for seeking access to an installation. (DoDM 5200.08 Vol 3)

REAL ID. A state issued driver's license or identification card meeting the security standards established by the REAL ID Act of 2005. (REAL ID Act of 2005)

Redress. A process for an individual to de-conflict his or her identity with that of another individual with whom they are frequently or easily mistaken (such as two individuals with similar names or similar identifiers, one with a criminal history and one without). Redress can be accomplished by providing additional biographic information to distinguish between the identities (such as a date of birth or social security number) or biometric information (such as fingerprints). Redress allows the proper identity to be evaluated for fitness. (DoDM 5200.08 Vol 3)

Site. For the purposes of this Order, Marine Corps installations, depots, training centers, facilities, and off-installation activities on land owned or leased by the Marine Corps.

Source Identity Document. A document that establishes that specific identity exists, though it does not associate that identity with a specific person. For example, a birth certificate or social security card. These documents may be used in conjunction with others to associate a specific person with a specific identity. (DoDM 5200.08 Vol 3)

Special Event. Planned time-bound activities (either one-time or recurring) that by their nature have a number of non-installation-assigned individuals attending, and are often characterized by a desire for mass public participation by individuals not otherwise eligible for recurring access to the installation. Examples include, but are not limited to, graduations, sporting events such as military academy football games, conferences, and public exhibitions. A special event by its very nature, or specific

statutory or regulatory authority, may warrant security, safety, and/or other logistical support or assistance. (DoDM 5200.08 Vol 3)

Trusted Traveler Access. A type of access where an individual is granted entry to the installation based on another authorized person's verification of their identity, fitness, and purpose. (DoDM 5200.08 Vol 3)

United States Identification Card (USID). Sometimes called the TESLIN or the Dependent or Retiree ID Card. Includes the DD Form 2 (Retired, Reserve, and Reserve Retired versions), DD Form 1173 and 1173-1, and the DoD Civilian Retiree Card as described by DoDI 1000.13 and Volumes 1 and 2 of DoDM 1000.13. (DoDM 5200.08 Vol 3)

Unescorted Access. A type of access where an individual is able to travel unaccompanied on an installation. (DoDM 5200.08 Vol 3)