PRIVACY IMPACT ASSESSMENT (PIA)

For the

Biometric and Automated Access Control System
United States Marine Corps (USMC)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐ **Yes, DITPR** Enter DITPR System Identification Number

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☒ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier NM05512–2 BADGE AND ACCESS CONTROL SYSTEM

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number | USMC Reports Manager, ARDB was contacted and determination was made that an OMB control number is not required.

Enter Expiration Date |

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 113; Secretary of Defense
10 U.S.C. 5013; Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 12333; United States Intelligence Activities
E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
National Defense Authorization Act of 2008, Section 1069
DoDD 8521.01E, Department of Defense Biometrics
DoDD 8500.1, Information Assurance
OPNAVINST 5530.14C, Navy Physical Security
Marine Corps Order 5530.14A, Marine Corps Physical Security Program Manual
AR 25-2, Information Assurance and E.O. 9397 (SSN), as amended.
Directive Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control"

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of this system is to enhance the identity management of DoD Persons and streamline business functions through a biometric database for designated populations. The following functions are the key processes supported by this system:

To support DoD physical security, force protection, identity management and access control missions by identifying and/or verifying an individual through the use of a biometric database for designated populations for the purpose of protecting U.S./Coalition/allied government/national security areas of responsibility and information.

To provide personnel identification and verification capabilities during disaster scenarios or other catastrophic events.

The United States Marine Corps (USMC) is augmenting security forces who support physical access control procedures for gaining access to USMC installations, through implementation of an electronic identity authentication system. The necessity exists to collect Personally Identifiable Information (PII) from participating DOD personnel, contractors and persons seeking access to a USMC installation and/or its facilities.

The Biometric and Automated Access Control System (BAACS), is to be initially used by DOD Active Duty, DOD Retirees, DOD Civilians, DOD contractors and visitors/VIPs.

The system is owned and operated by the USMC Plans, Policy and Operations (PP&O), who furnishes the Commercial off the shelf (COTS) hardware and software for the system. PP&O through the USMC host installation's Provost Marshal's Office (PMO), is responsible for collecting, storing and protecting PII of personnel who enroll in the system. PMO enrolls the PII in the BAACS and the system is used to electronically authenticate the identity of personnel who are seeking access to USMC installations. PP&O and the PMO share no PII beyond the authority (statutory or otherwise) specified in this document.

Initially, DOD personnel participation in the system is voluntary. However, individual USMC installation commands have the authority to identify groups of personnel that may be required to use the system.

The system supports three functions: (1) Enrollment, (2) Credentials, (3) Physical Access Control.

Currently the system is in the design stage and is scheduled to be implemented at U.S. Marine Corps Base Camp Pendleton in the 2nd Quarter of Fiscal Year 2010. However, this PIA will cover deployments of the system at additional USMC installations across the Continental United States (CONUS).

Types of personally identifiable information collected:

The USMC PMO collects certain Biometric information directly from active duty or retired DOD service members, DOD civilians and contractors as well as visitors and vendors. The USMC PMO uses this information to manage and provide the physical access control to the installation, electronic identity authentication and background screenings.

The information collected by the USMC PMO consists of the following:
• Name
• Service affiliation
• Unit
• Unique Identifier (e.g. PIV card unique identifier, Global Unique Identifier and/or system code unique identifier)
• Personal Identity Verification (PIV) card information
• Social security number (only in non-routine instances - see ** below)
• Telephone Number

The Biometric information collected by the USMC PMO consists of the following:
• Digital photograph of face
• Digital fingerprint images
• Digital Vascular Pattern images of hand(s)
• Digital Iris images
• For all Biometric information collected, images are collected and converted to template format, then the templates are stored in the system. No images are stored in the system.

** The USMC PMO may also collect from the person, their Social Security Number, however, this collection may not be required if the forms of identification are deemed satisfactory or if the person has an existing DOD Common Access Card (CAC) or TESLIN PIV card that is verifiable via the DOD Defense National Visitor Center (DNVC). Persons are not eligible to use the system if they do not provide the required information. The host USMC installation's Commander and PMO has sole authority for granting or denying the person access to use the system or to access the installation via an alternative process.

In addition, during the enrollment process, the installation requires that individuals who do not hold a CAC or TESLIN PIV card (visitors) must present acceptable I-9 documentation (provided in the Appendices to the BAACS PIA as Appendix A) to verify identity. The USMC Installation's PMO reviews but does not collect copy or store these identification documents.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The risks associated with the PII data collected by the BAACS include:

a. The existence of the system is a risk. It contains personal identity information about individuals that includes their personal information and Biometric records. The information collected is used to operate the system including conducting electronic identity authentication of persons who volunteer to enroll and use the system. An important element of the system is that currently, participation is voluntary. Persons who are concerned about the privacy implications of providing the PII necessary to be used by the system are able to choose not to use the system and instead use the installation's alternate access procedures.

In addition, to allay concerns of private citizens who may not wish to share their PII with the government, the system has been designed to limit the amount of PII that the USMC PMO collects and stores. For purposes of the USMC PMO's collection, use and storage of PII, persons have broad privacy protections accorded to them under applicable laws. Persons also have a contractual relationship with the USMC PMO through a User Agreement (provided in the Appendices to the BAACS PIA as Appendix C) , which imposes obligations upon the USMC PMO to maintain privacy safeguards. The USMC installation is mandated by federal law (i. e. the Privacy Act) to maintain privacy protections of a person's PII.

b. The system is designed to allow for collection of only those personal data elements necessary to allow the USMC PMO to perform their physical security and installation access control tasks. The USMC PMO collects only individual information needed to perform electronic identity authentication for physical access to USMC installations/facilities and to prepare the system visitor credential. The USMC PMO authorizes only a limited number of its personnel to receive password-protected access to the PII to review the details of individual person's enrolled data.

c. The system logs and records times, dates and locations where users access the installation, so the system can be used to track the access activity of users. The USMC PMO regularly provides to the installation's USMC PMO access control manager representative, PII that consists of the person's name and the date, time and location reflecting that the individual has utilized the system to gain access to the USMC installation. The USMC PMO authorizes only a limited number of its personnel to receive password-protected access to the PII to review the details of individual person's access history reports.

d. Biometric images are not stored in the system. At the time of enrollment, a user's Biometric is scanned; an image is created but is not saved or stored, and is only used to create the user's Biometric templates, which are subsequently stored in the system database.

e. The system is not used to electronically initiate or process background screening nor does the system store or

collect results of back ground screening.

f. The system security controls have not yet been tested. This risk will be mitigated by testing the security controls as part of the DIACAP. The PIA will be updated to reflect test results. The USMC PMO employs the principle of least-privilege access and uses strong encryption on PII, and encrypts its entire database backups to protect the data.

Individual social security numbers and Biometrics are encrypted prior to being placed in the USMC PMO's database. PII collected during enrollment is not temporarily stored on the enrollment station and is transmitted in encrypted form to the USMC PMO's Data Center.

The system is designed to provide for secure transmission of PII through encryption, Secure Socket Layer (SSL) and other secure IT to minimize the risk of data loss or interception. The USMC PMO's database is a stand-alone system that is not connected to any public networks, but is will utilize infrastructure of the MCESS ATFP network at USMC Base Camp Pendleton, CA. The USMC PMO securely transmits PII data using FIPS 140-2-validated encryption technology to send information to and from the USMC PMO's data center. Non-USMC PMO entities do not have logical access (i.e., connection of computer systems or networks) to the BAACS database. Individual information on the BAACS database is secured consistent with applicable federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need-to-know policy. Physical access to the system and private database is controlled with the use of PIV credentials. The system and the databases are housed in controlled data centers within secure facilities.

g. Loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of PII are all risks.

The USMC requires the USMC PMO to meet stringent criteria for maintaining the privacy and security of all PII data in its database, which are based on the NIST standards 800-53 Federal Information Processing Standards (FIPS) 199. By requiring the USMC PMO to meet these criteria, the USMC minimizes any attendant privacy risks associated with the handling of PII.

All DoD employees and contractors are required to take mandatory security and privacy training prior to accessing a DoD system. This security and privacy training course includes an overview on privacy and personally identifiable information and its appropriate uses. Further, all actions on the system are logged and maintained to ensure accountability.

Access Control: USMC PMO will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training: USMC PMO will: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability: USMC PMO will: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments: USMC PMO will: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management: USMC PMO will: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning: USMC PMO will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication: USMC PMO will identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response: USMC PMO will: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: USMC PMO will: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection: USMC PMO will: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection: USMC PMO will: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: USMC PMO will develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security: USMC PMO will: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment: USMC PMO will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition: USMC PMO will: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection: USMC PMO will: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity: USMC PMO will: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. The USMC PMO regularly provides to the host installation's USMC PMO access control manager representative, PII that consists of the person's name and the date, time and location the individual has utilized the system to gain access to the USMC installation.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Persons initiate the collection and maintenance of their PII when they enroll with the USMC PMO to use the system. Participation in the Biometric and Automated Access Control System, and therefore the submission of individual information, is voluntary, until such time that the DOD or host USMC installation commanding officer issues policy that states otherwise or results in the USMC's determination that the collection and maintenance of PII is a requirement that facilitates compliance with DOD or command policy. Persons who choose not to provide their PII for the system may be denied access to the installation or may be granted access to the installation, however, they shall be bound by the alternate access procedures specified by the host USMC installation's PMO.

A comprehensive written notice, referred to as a User Agreement, is provided to, and is required to be read by, persons at the time of system enrollment. The User Agreement explains what information is being collected, why it is being collected and what uses will be made of the information. The User Agreement is presented at the USMC PMO enrollment station before the enrollment process begins. Persons are required to read the User Agreement in its entirety and to consent to its terms, in order to proceed with enrollment. Persons must sign a consent form to affirm their consent to the terms of the User Agreement. After giving this consent, the enrollment administrator begins the enrollment. The User Agreement informs persons that, if they do not agree to all terms, which include collection and use of their individual information, they should select the "I do not agree to the terms" entry and terminate the enrollment process. Persons do not have the right to selectively consent to provide some, but not all, of the individual information they are required to provide in order to enroll for the system.

Further, any workstation of the BAACS that has the capability to collect or display personal information, either via PIV card reader, user data entry, or attached Biometric collection device, shall have a Privacy Act Statement overtly displayed.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The USMC's ability to protect the buildings, grounds, and property that are owned or occupied by the USMC and/or other DOD or federal agencies and the USMC's ability to protect and ensure the safety and security of personnel within such property is not achievable if individual persons are authorized to consent to specific uses of their PII.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☒ **Other** ☐ **None**

Describe each applicable format.	Before information is collected, the individual is provided the opportunity to read the Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), and the User Agreement thereby allowing an individual to make an informed decision about providing the data. The User Agreement, is provided and required to be read by, persons at the time of system enrollment. The User Agreement explains what information is being collected, why it is being collected and what uses will be made of the information. The Statement advises that participation is voluntary and individuals will have an

opportunity to decline participation, however, failure to provide requested information may result in denial of access to benefits, privileges, and DoD installations, facilities, buildings, computer systems and networks. Individuals who choose to participate will offer implied consent to collection of information by their actions, such as voluntarily offering their CAC for usage, voluntarily offering their fingerprints, irises, and facial profiles for image collection.

PRIVACY ACT STATEMENT
AUTHORITY
5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Navy; 10 U.S.C. 8013, 10 U.S.C. 5041, Headquarters, Marine Corps; 50 U.S.C. 797, Security Regulations and Orders; Homeland Security Presidential Directive-12, Policy for a Common Identification Standard for Federal Employees and Contractors; Homeland Security Presidential Directive-24, Biometrics for Identification and Screening to Enhance National Security; Department of Defense Directive 8500.1, Information Assurance (IA); DoD Directive 8521.01E, Department of Defense Biometrics; Army Regulation 25-2, Information Assurance; SECNAV M-5239.1, Information Assurance Manual; AFI 33-202, Network and Computer Security; and E.O. 9397, Numbering System for Federal Accounts Relating to Individual Persons.

PRINCIPAL PURPOSE(S)
To control physical access to Department of Defense (DoD) and USMC controlled installations and facilities and to support the DoD physical and logical security, force protection, identity management, and personnel recovery, by identifying an individual or verifying/authenticating the identity of an individual through the use of Biometrics (i. e. measurable physiological or behavioral characteristics) for purposes of protecting U.S./Coalition/allied government and/or U.S./Coalition/allied national security areas of responsibility and information.

ROUTINE USE
To Federal, State, tribal, local, or foreign agencies, for the purposes of law enforcement, counterterrorism, immigration management and control, and homeland security as authorized by applicable U.S. Law or Executive Order, or for the purpose of protecting the territory, people, and interests of the United States of America against terrorist activities and breaches of security related to DoD- controlled information, facilities, and installations. The “Blanket Routine Uses” set forth at the beginning of the Navy’s compilation of System of Records Notices apply to this system.

DISCLOSURE
Voluntary. However, failure to provide requested information may result in denial of access to DoD installations, facilities, and buildings.

User Agreement (provided in the Appendices to the BAACS PIA as Appendix C):
A comprehensive written notice, referred to as a User Agreement, is provided to, and is required to be read by persons at the time of system enrollment. The User Agreement explains what information is being collected, why it is being collected and what uses will be made of the information. The User Agreement is presented at the USMC PMO enrollment station before the enrollment process begins. Persons are required to read the User Agreement in its entirety and to consent to its terms, in order to proceed with enrollment. Persons must sign a consent form to affirm their consent to the terms of the User Agreement. After giving this consent, the enrollment administrator begins the enrollment. The User Agreement informs persons that, if they do not agree to all terms, which include collection and use of their individual information, they should select the "I do not agree to the terms" entry and terminate the enrollment process. Persons do not have the right to selectively consent to provide some, but not all, of the individual information they are required to provide in order to enroll for the system.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.