PRIVACY IMPACT ASSESSMENT (PIA)

For the

Base Pass and Access Control (BPAC)
Department of the Navy - 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

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

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. 5013, Secretary of the Navy;
10 U.S.C. 5041, Headquarters, Marine Corps;
OPNAVINST 5530.14C, Navy Physical Security;
Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual.

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.

Under the new directives and policies cited in 2(f) above, the Provost Marshal's Office (PMO) has additional responsibilities for controlling a multitude of passes issued through a variety of organizations. Consolidating access control under a central PMO will result in a significant increase in the number of passes PMO will generate, track, and account for. The preponderance of locally issued passes are issued to local nationals residing in Okinawa, Japan. The current process is manually driven, inefficient, and relies on a cumbersome filing system. In addition, the current passes are manually produced, are of low quality, easily replicated and/or altered.

The purpose of the new solution called BPAC (Base Passes and Access Control) is to enhance installation security, improve ability to manage, update, and account for passes issued.

BPAC will collect the following PII Data:

1. Name: Last, First, Middle
2. Gender
3. Descriptive information, i.e.: Height, weight, eye and hair color
4. Date and Place of Birth
5. Citizenship/Nationality
6. Permanent Address
7. Present Address
8. Biometrics (fingerprint scan)

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

There is, and always will be the risk of compromise when PII data is collected. The compromise could be because of honest human errors or as a result of exploitation of vulnerabilities in the system, methods, and/or data stores. Certain pieces of PII data if revealed by mistake or by security exploit, together could establish a pseudo identity of the owner of data which when supplemented by other PII data or publicly available information such as address and phone number etc... enables a person in possession of this PII data to steal the identity of legitimate data owner. There are a variety of scenarios in which the privacy of the data owner could be compromised resulting in potential harm to the owner of data as well as to the legitimate user of such data. Potential risks of privacy must be mitigated by using self-defensive mechanism in the system and improvements in data accessibility, security, storage and use methods that can mitigate the potential risks while maintaining the Confidentiality, Integrity, and Availability (CIA)of data for legitimate usage.

The risk of preserving PII data while in the system and on mobile devices is assured by following NIST standards recommended in HSPD-12 Guidelines. The following standards and guidelines are used to ensure the protection of PII data, and reduce the vulnerabilities in the system that could be compromised:
1. NIST FIPS 201-1
2. NIST SP 8500-B
3. NIST SB 2006-01
4. NIST SB 2005-03
5. STIGs
6. NIST 800-111 (Guide to Storage Encryption Technologies for End User Devices) [Hand Held Scanners in BPAC]
In addition, access to PII data will be protected on hand held devices which has higher potential of data loss because of human error. All PII data fields will be encrypted, only a subset of the data required to accomplish vetting of data owner will be loaded onto the handheld devices. The handheld devices are hardened with an embedded version of Windows CE that is only employing the necessary services required for accomplishing the task of credential vetting. Identity of the legitimate user will be established using a combination of security levels (What do you know? What do you have? and/or Who are you?)

On the server, the Windows Server 2008 and Microsoft SQL Server 2008 will be hardened using STIG's, and NIST Security guidelines and the PII data elements will be stored encrypted. Similar to mobile scanners, combination of security levels will be used before granting access to PII data on the server. The terminals that will be used to access PII data will have hardened version of Windows XP that are only employing the services required for system function.

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. Department of the Navy: USMC Provost Marshal's Office, Accident Investigation Section, Criminal Investigation Division; Naval Criminal Investigative Service; Navy Military Police

☒ **Other DoD Components.**

Specify. Air Force and Army Military Police

☐ **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.

Individuals may object to the collection verbally or by refusing to sign the Base Pass Application form, however they will not be able to access the base.

(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.

Individuals sign our Base Pass Application form that contains the following informational statements: Authority, Purpose, Routine Uses, Disclosure is Voluntary and Privacy Act. In the "Disclosure is Voluntary" statement, it is explained to the customer they will not receive base access if they do not provide the required information.

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

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.

The following statement is on the Base Pass Application sheet:
AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; OPNAVINST 5530.14C, Navy Physical Security; Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual.
PRINCIPAL PURPOSE: To maintain all aspects of proper access control; to issue passes, replace lost passes and retrieve passes upon separation; to maintain visitor statistics; collect information to adjudicate access to facility; and track the entry/exit times of personnel.
ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) to designated contractors, Federal agencies, and foreign governments for the purpose of granting Navy officials access to their facility.
DISCLOSURE IS VOLUNTARY: Failure to disclose the information will result in the individual not being processed for or receiving installation access.
PRIVACY ACT - 1974 as Amended applies: This memo may contain information which must be protected IAW DoDD 5400.11, and it is For Official Use Only (FOUO).

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.