PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel Accountability System (PAS)
Department of the Navy - Commander, Navy Installations Command

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 DADMS ID: 80546

☐ **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, NM5000-2

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.

SORN authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program
Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual
E.O. 9397 (SSN), as amended.

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 the Personnel Accountability System (PAS) is to automate shipboard and shore-based personnel accountability functions with a high degree of efficiency and security. The PAS employs a fingerprint reader, Smartcard reader, and a barcode scanner to perform automated "check-in/check-out" procedures for personnel who possess a compatible smartcard (either a Department of Defense Common Access Card (CAC), a Transportation Worker Identification Credential (TWIC), a Defense Biometric Identification System (DBIDS) card, or a GSA Personal Identity Verification II (GSA PIV II) Smartcard). In addition, the PAS suite may include a fingerprint scanner, associated fingerprint matching algorithms, and a biometrics storage capability that can enable an individual's fingerprints and photograph to be entered into the PAS database. The biometric features of PAS enables the accountability procedures currently in use for smartcard holders to be augmented with additional layers of security (i.e, personal identify verification through the use of stored fingerprints and facial images.) The PAS biometric accountability features can be be used either independent of or in conjunction with the system's card reader and barcode scanner.

Purpose from DITPR DON: To control physical access to DoD, Department of the Navy (DON) or U.S. Marine Corps Installations/Units controlled information, installations, facilities, or areas over which DoD, DON or USMC has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./Coalition/allied government/ national security areas of responsibility and information; to issue badges, replace lost badges and retrieve passes upon separation; to maintain visitor statistics; collect information to adjudicate access to facility; and track the entry/exit times of personnel.

The types of personal information about individuals collected by the PAS include: Full name; social security number (SSN) (optional) or DoD ID Number; Navy/Marine Corps base/activity/contractor facility; service branch, rank, pay grade, rating/occupation; Unit Identification Code (UIC); command/battalion; division/ platoon; department/company; duty section; home/work address; home/work e-mail address; home/work/ mobile/phone numbers; digital prints of right and left index fingers; and digital facial image.

Note: Home address, e-mail addresses and phone numbers are used if there is a need to contact the individual. E-mail addresses may be business or personal. Phone numbers may be home, cellular, or business contact numbers. Biometrics are used to identify the individual. Other PII collected includes branch of service, pay grade, and rating/occupation that are used by the commanding officer. PAS has three options for the collection of SSN, required, optional, or not allowed. The selection of an option can be based on the individual needs of the component/site/command that is using PAS. If the not allowed option is selected, all SSNs are removed from the database. The choices regarding SSN allow sites the ability to comply with the SSN Reduction Plan when required. The collection of the DOD Id number identifier can be used in place of the SSN.

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

The access, storage, and transmission of the PII collected by the PAS is subject to various privacy risks. The primary privacy risks to the PII collected by PAS include: the intentional misuse of PII by administrative users; the physical compromise of the PAS PII database; and the loss or theft of PAS laptop computers and the data they contain.

To mitigate these privacy risks the PII database associated with the PAS is encrypted both at rest and while in transit. Only designated administrative users with the "need to know" can access the full PII database. In addition, secure log on procedures for administrative users require either positive fingerprint authentication or authentication through smartcard and PIN combinations. Regular PAS users must also utilize secure log on procedures to access the system. However, the regular users can only view a lower level of PII that is contained in the check-in/check-out screen (name, branch of service, rank, UIC, department/company, division/platoon, liberty risk, and "buddy group" information.) All PAS users are required to complete annual PII awareness training. In addition, the PAS includes

an "Events Report" feature that logs system usage and provides a means of auditing the activities of all users.

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. Within, not between, the U.S. Navy and Marine Corps commands using the application

☒ **Other DoD Components.**

Specify. Within, not between, the Army and Air Force commands using the application

☐ **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.

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

PII is not collected directly from the individual. PII is obtained from the individual's smart card and a fingerprint scanner. The Commanding Officer (CO) is ultimately responsible for the security of his or her command. The PAS is a tool that a CO may elect to use to improve the process of identifying, validating, and accounting for personnel entering and departing the areas under his or her cognizance. The Commanding Officer has the authority to implement the use of PAS, and to require that the necessary PII from the smart card and fingerprint scanner be provided by the personnel assigned to the command or by anyone being tracked by the PAS.

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.

PII is not collected directly from the individual. PII is obtained from the individual's smart card and a fingerprint scanner. The Commanding Officer (CO) is ultimately responsible for the security of his or her command. The PAS is a tool that a CO may elect to use to improve the process of identifying, validating, and accounting for personnel entering and departing the areas under his or her cognizance. The Commanding Officer has the authority to implement the use of PAS, and to require that the necessary PII from the smart card and fingerprint scanner be provided by the personnel assigned to the command or by anyone being tracked by the PAS.

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.

PII is not collected directly from the individual.

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.