**PRIVACY IMPACT ASSESSMENT (PIA)**

**PRESCRIBING AUTHORITY:** DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. **DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:**
   - Personnel Accountability System (PAS)

2. **DOD COMPONENT NAME:**
   - Department of the Navy

3. **PIA APPROVAL DATE:**
   - 06/18/18

4. **Bureau of Naval Personnel (BUPERS)**

**SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)**

a. **The PII is:** (Check one. Note: foreign nationals are included in general public.)
   - From members of the general public
   - From both members of the general public and Federal employees and/or Federal contractors
   - Not Collected (if checked proceed to Section 4)

b. **The PII is in a:** (Check one)
   - New DoD Information System
   - Existing DoD Information System
   - New Electronic Collection
   - Existing Electronic Collection

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 identity 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.

The types of personal information about individuals collected by the PAS from the individuals CAC or other credential includes: Full name; 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 default is "not allowed" and the new Memorandum of Understanding (MOA) states the receiving sites will NOT collect SSN data. 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 collection of the DOD ID number identifier is used in place of the SSN. If the MOA should change to allow the collection of the SSN at some future time then the PIA will be updated.

d. **Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)**

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 be provided by the personnel assigned to the command or by anyone being tracked by the PAS.

e. **Do individuals have the opportunity to object to the collection of their PII?**
   - Yes [X]
   - No
(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

| PII is not collected directly from the individual. PII is obtained from the individual's smart card and is necessary for the specific access required. 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 be provided by the personnel assigned to the command or by anyone being tracked by the PAS. |

<table>
<thead>
<tr>
<th>f. Do individuals have the opportunity to consent to the specific uses of their PII?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

(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. Consent is assumed based on the issuance of the individual's CAC. |

| g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.) |
|---|---|---|
| Privacy Act Statement | Privacy Advisory | Not Applicable |

| PII is not collected directly from the individual. A Privacy Act Statement is completed by each employee/individual when they are initially issued their CAC. |

| h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check 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 (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.) | Specify. |
| Other (e.g., commercial providers, colleges). | Specify. |

| i. Source of the PII collected is: (Check all that apply and list all information systems if applicable) |
|---|---|
| Individuals | Specify. |
| Databases | Specify. |
| Existing DoD Information Systems | Specify. |
| Commercial Systems | Specify. |
| Other Federal Information Systems | Specify. |

| The source of the PII is an individual's smart card or Common Access Card (CAC). After visual identification and authentication by the PAS authorized administrator, the individual's smart card is inserted into a card reader, and the smart card information is automatically entered into the PAS database for verification and identification. To facilitate identification and authentication, fingerprints from the individual may also be collected via a fingerprint reader connected to the PAS. There are no connections between the PAS and other databases or systems. |
j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- E-mail
- Face-to-Face Contact
- Fax
- Information Sharing - System to System
- Other (If Other, enter the information in the box below)

All PII data is collected from the user's CAC.

k. 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 must be consistent.

- Yes [x]
- No

If "Yes," enter SORN System Identifier

NM05512-2, NM05000-2

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

- N1-NU-89-4

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

SSIC 5512-2a. Temporary. Generally, destroy when no longer needed, i.e., when superseded or after member's transfer. Longer retention is authorized if required for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

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

(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII.

- Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

- If direct statutory authority or an Executive Order does not exist, indirect statutory 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.

- If direct or indirect authority does not exist, 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 must be identified.

SORN NM05512-2, Badge and Access Control System Records (April 09, 2014, 79 FR 19593), authorities:


SORN NM05000-2, Program Management and Locator System (January 24, 2008, 73 FR 4193), authorities:
10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN), as amended.

**II. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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
- [x] No
- [ ] Pending

1. If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
2. If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
3. If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

PAS does not collect PII from members of the public.