**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:**
   SPAWAR Enterprise Information Technology Service Management (SEITSM)

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

3. **PIA APPROVAL DATE:**
   02/03/20

**Naval Information Warfare Center (NIWC) Atlantic**

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

<table>
<thead>
<tr>
<th>a. The PII is: (Check one. Note: foreign nationals are included in general public.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ From members of the general public</td>
</tr>
<tr>
<td>☐ From both members of the general public and Federal employees and/or Federal contractors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>b. The PII is in a: (Check one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗ New DoD Information System</td>
</tr>
<tr>
<td>☐ Existing DoD Information System</td>
</tr>
</tbody>
</table>

| ☐ Significantly Modified DoD Information System |

<table>
<thead>
<tr>
<th>c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.</th>
</tr>
</thead>
</table>

The SPAWAR Enterprise Information Technology Service Management (SEITSM) System is built utilizing BMC Software Inc's IT Service Management (ITSM) suite of applications. This suite consists of BMC Remedy ITSM Service Desk (Incident and Problem Management), Change Management (including Release), Asset Management, Service Level Management, Service Request Management, Knowledge Management, Analytics, Reporting Dashboards, and other enabling technologies. SEITSM is used to manage IT support for a wide range of Navy/Marine Corps systems; ranging from Pay and Personnel systems to Fleet C4I systems. The SEITSM system enables the command end users to document, prioritize, track, and generate metrics based on the information entered into the ITSM suite modules. Data is entered into the system by the Tier 1 support staff and support technicians (Tier 2 and Tier 3 users). Reports and metrics are generated from the system and distributed to management personnel as well as the users (PII data is not available for reporting). The system is administered by the SEITSM development staff and the New Orleans Data Center staff. The system has three interfaces (PII data is not shared through any interfaces); the SPAWAR Acquisition & Integrated Logistics Online Repository (SAILOR) system, the Navy 311 system, and the ticketing system for the Mobile User Objective (MUOS) system.

The PII information collected is:
- Name (Last, First, MI)
- SSN # (full or partial)
- Date of Birth
- Place of Birth
- Official Duty Telephone #
- Official Duty Address
- Work Email Address
- Rank/Grade
- DOD ID Number
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)*

Administrative Use.
SSN is collected from DoN personnel to allow queries of pay/personnel records to correct pay/personnel issues on personnel that are supported by the Naval Information Warfare Center (NIWC) Enterprise Service Desk. Supported programs are Naval Reserve Order Writing System (NROWS), Navy Standard Integrated Personnel System (NSIPS), Defense Travel System (DTS), Career Management System - Interactive Detailing (CMS-ID), Medical Readiness Reporting System (MRRS), Defense Joint Military System - Active Component (DJMS-AC), Defense Joint Military System - Reserve Component (DJMS-RC).

SSN, DOB, and POB are collected from DoN contractor and government personnel for onboarding to NIWC Atlantic. This information is used to create electronic applications for DoD Common Access Card (CAC), and to verify security clearance data in the JPAS system.

e. Do individuals have the opportunity to object to the collection of their PII?  
   (X) Yes  ☐ 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.

The individual end user has the right to refuse to provide his/her SSN. The inquiry is normally via a telephone call to the help desk, so when the Support Center Analyst informs the end user that his/her SSN is required in order to further assist them, if the person refuses to provide it, then they are informed that the Enterprise Service Desk (ESD) will not be able to proceed further without the SSN.

f. Do individuals have the opportunity to consent to the specific uses of their PII?  
   (X) 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 majority of legacy systems that are used to conduct record changes, pay modifications, etc are maintained by the end user's SSN. Once a caller's issue is identified by the SCA and the SSN is required, the SCA informs the caller that the SSN is needed in order to conduct the proper research and to access the required records. If the caller does not wish to provide the SSN, the SCA informs him or her that they will be unable to proceed further with assisting them with their request.

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.)*

(X) Privacy Act Statement  ☐ Privacy Advisory  ☐ Not Applicable
Authority: N07220-1; 10 U.S.C. 5013. Secretary of the Navy and E.O. 9397 (SSN), as amended.

Purpose: The purpose of this system is to provide secure worldwide personnel and pay support for Navy members and their commands. To allow authorized Navy personnel and pay specialists to collect, process, modify, transmit, and store unclassified personnel and pay data. Additionally, the system supports management of leave and pay entitlements and deductions so that this information can be provided to the Defense Finance and Accounting Service (DFAS) for payroll processing. The system also supports collection of spouse and child information to be used for updates to the military member's dependency status.

Routine Use(s): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The DoD Blanket Routine Uses that appear at the beginning of the Navy's compilation of system of records notices may apply to this system.

Disclosure: Disclosure of requested information is voluntary; however, failure to provide such information may result in denial of request.


Purpose: To provide a DoD-wide travel management process which will cover all official travel, from pre-travel arrangements to post-travel payments, to include the processing of official travel requests for DoD personnel, and other individuals who travel pursuant to DoD travel orders; to provide for the reimbursement of travel expenses incurred by individuals while traveling on official business; and to create a tracking system whereby DoD can monitor the authorization, obligation, and payment for such travel.

To establish a repository of archived/Management Information System (MIS) travel records which can be used to satisfy reporting requirements; to assist in the planning, budgeting, and allocation of resources for future DoD travel; to conduct oversight operations; to analyze travel, budgetary, or other trends; to detect fraud and abuse; and to respond to authorized internal and external requests for data relating to DoD official travel and travel related services, including premium class travel.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To Federal and private entities providing travel services for purposes of arranging transportation and lodging for those individuals authorized to travel at government expense on official business. To the Internal Revenue Service to provide information concerning the pay of travel allowances which are subject to federal income tax. To banking establishments for the purpose of confirming billing or expense data.

The DoD ‘Blanket Routine Uses’ set forth at the beginning of the DoD compilation of systems of records notices apply to this system.

Disclosure: Disclosure of requested information is voluntary; however, failure to provide such information may result in denial of request.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- [x] Within the DoD Component
  - Specify. Naval Information Warfare Center (NIWC) Atlantic government personnel with a need to know.
- [ ] Other DoD Components
- [ ] Other Federal Agencies
- [ ] State and Local Agencies
- [ ] 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)

- [x] Individuals
- [ ] Databases
- [ ] Commercial Systems
- [ ] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Other Federal Information 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)

- Official Form (Enter Form Number(s) in the box below)
- Paper
- Telephone Interview
- Website/E-Form

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
- No

If "Yes," enter SORN System Identifier: N07220-1; DHRA 08 DoD

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

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. DAA-NU-2015-0005-007

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

(3) Retention Instructions.

SSIC: 5000.2 - Record Schedule: 5000-82
TEMPORARY: Cutoff at end of calendar year. Destroy 3 years after cutoff.

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. (If multiple authorities are cited, provide all that apply).
   (a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
   (b) 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.
   (c) 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 N07220-1, Navy Standard Integrated Personnel System (NSIPS) (November 29, 2012), 77 FR 71185, authorities:
10 U.S.C. 5013, Secretary of the Navy and E.O. 9397 (SSN), as amended
DHRA 08 DoD, Defense Travel System (March 24, 2010, 75 FR 14142)

Other authorities:
n. 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  ☒ 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.

This DoD information system does not collect information from members of the public.