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:

NAVSUP Enterprise Web Portal

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

06/05/23

Headquarters, Naval Supply Systems Command

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 Federal employees and/or Federal contractors
- [x] 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
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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.

The NAVSUP Enterprise Web Portal is the combined web presence for Naval Supply Systems Command. It consists of the NAVSUP Public Website, MyNAVSUP Employee Intranet, and approximately 115 custom developed applications to enhance productivity within NAVSUP and to support logistics processes that are not handled by other systems. The NAVSUP Enterprise Web utilizes an Identity Management Suite to authenticate users for NAVSUP IT systems. Completed instances of DD Form 577 (Appointment/Termination Record) are maintained for NAVSUP employees who can approve travel requests and travel vouchers within the Defense Travel System (DTS). The NAVSUP BSC Human Capital Strategy (HCS) application collects information on employees to facilitate the organization in identifying personnel for future projects.

PII is collected from all users registering within my.navsup.navy.mil. Information from the Common Access Card (CAC) and embedded PKI Certificates is used for user identification and determination of access to NAVSUP Information Technology Systems. The PII that is collected from all users registering within my.navsup.navy.mil are: name, citizenship status, registrant type (Military/Civilian/Contractor) and DoD ID Number.

PII collected and/or maintained, as applicable for specific sub systems and applicable users within the NAVSUP Enterprise includes: User names, grade, organization, Electronic Data Interchange Personal Identifier (EDIPI), address for the employee's telework location, phone number, activity, billet identification number, General Schedule (GS) job series, step level, position description number, gender, date of birth, height, weight, and eye color, employee's name, DoD ID Number, citizenship status, and registrant type (military/civilian/ contractor).
PII is collected within the EEO application that include details of discriminatory instances and other details of the discriminatory act. The EEO application also collects information pertaining to reasonable accommodations.

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 PII collected and/or maintained within NAVSUP Enterprise Web is used for a number of purposes. The NAVSUP Enterprise Web portal utilizes an integrated identity management solution that collects PII for the identification and authorization of users. Additional applications and processes utilize PII for a number of different purposes such as administrative use, verification purposes, and mission-related uses. PII collection is kept to a minimum, but allows enough information for an informed approval to be made concerning technical and physical accesses, travel privileges, telework, and other cases where PII is needed to make a determination for the betterment of the individual and/or organization. PII collection is necessary to maintain records required by law.

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.

Users have the opportunity to object to the collection of their PII by refusing to provide their PII to the system or forms collecting/requesting the information. Objecting to the collection of PII may negatively affect technical and physical accesses, travel privileges, telework, and other cases where PII is needed to make a determination for personnel.

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.

Users have the opportunity to object to the specified use of their PII by refusing to provide their PII to the system or forms collecting/ requesting the information. Objecting to the specified use of PII may negatively affect technical and physical accesses, travel privileges, telework, and other cases where PII is needed to make a determination for personnel.

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

Privacy Act Statement

AUTHORITY: 5 U.S.C. Section 301 Departmental Regulations. Information required to assist officials and employees of the Navy in the management, supervision, and administration of Navy personnel and the operations of related personnel affairs and functions and personnel doing business with Navy. DoD Instruction 8510.01 Risk Management Framework for DoD Systems.

PURPOSE: Collect information on users of Naval Supply Systems Command (NAVSUP) Information Technology Systems as required for authentication of users and for role based access control. Information is collected on NAVSUP Employees for organizational planning and licensing of operators as required.

ROUTINE USES: Information will be used by the NAVSUP Business Systems Center staff to record registered users for NAVSUP Information Technology Systems. Information System Administration personnel will also review the user registration information for role based access. Employee Supervisors and HR personnel will use the information for organizational planning and employee hiring and human resources management.

DISCLOSURE: Voluntary; Users have the opportunity to object to the specified use of their information by refusing to provide their information to the system or forms collecting/requesting the information. Objecting to the specified use of personal information may negatively affect technical and physical accesses, travel privileges, telework, and other cases where PII is needed to make a determination for personnel.

LINK to SYSTEM OF RECORDS NOTICE:
https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/NavyUSMC-Article-List/

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.	Military Service Members and Civilian Personnel.
[ ] Other DoD Components	Specify.	
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	

[X] 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. Contractor Names: JMA Resources and C3 Innovations

A separate contract clause is included in the respective contracts regarding Privacy Act considerations. The contract clause requires the contractor to safeguard all privacy information, and ensure this data is accessed and maintained in accordance with applicable laws and regulations. If contractor access occurs to Privacy Act Information occurs, FAR 52.224-1 Clause (Privacy Act Notification) and 52.224-2 Clause (Privacy Act) apply.

[ ] 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
[X] Existing DoD Information Systems
[ ] Other Federal Information Systems
[ ] Databases
[ ] Commercial Systems

Navy ERP, Navy Total Workforce Management Services (TWMS)

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
[X] Information Sharing - System to System
[ ] Other *(If Other, enter the information in the box below)*
[X] Official Form (*Enter Form Number(s) in the box below)*
[ ] Paper
[ ] Telephone Interview
[X] Website/E-Form

DD 577 Form Appointment/Termination Record, FLCPH FORM 10490.1-5 (Rev. 10.12) - Application for MHE Operator License.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier N05200-1

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.

Original SORN package submitted on 5/29/2018. 04/08/2022 is the date the SORN request was submitted to the DON OPNAV DNS-36 Office. The SORN package is still being reviewed.

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. GRS 1.1: Financial Management and Reporting Records; GRS 1.3:

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

(3) Retention Instructions.

Data owners should adhere to the following retention instructions:
DAA-GRS-2016-0013-0001 (Financial Management and Reporting Records - Financial management and reporting administrative records): Destroy when 3 years old, but longer retention is authorized if needed for business use.

DAA-GRS-2015-0006-0001 (Budgeting Records): Destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use.
DAA-GRS-2017-0011-0001 (Employee Acquisition Records - Job vacancy case files): Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later.
DAA-GRS-2017-0007-0001 (Employee Management Records - Employee management administrative records): Destroy when 3 years old, but longer retention is authorized if required for business use.
DAA-GRS-2017-0007-0002 (Employee Management Records - Workforce and succession planning records): Destroy 3 years after issuing each new plan, but longer retention is authorized if required for business use.
DAA-GRS-2017-0007-0003 (Employee Management Records - Employee Incentive Award): Destroy when 2 years old or 2 years after award is approved or disapproved, whichever is later, but longer retention is authorized if required for business use.
DAA-GRS-2018-0002-0012 (Employee Relations Records - EEO discrimination complaint case files): Destroy 3 years after resolution of case, but longer retention is authorized if required for business use.
DAA-GRS-2016-0014-0001 (Employee Training Records) - Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.
DAA-GRS-2016-0016-0001 (Common Office Records) - Destroy when business use ceases
DAA-GRS-2016-0011-0001 (Facility, space, vehicle, equipment, stock, and supply administrative and operational records) - Destroy when 3 years old or 3 years after superseded, as appropriate, but longer retention is authorized if required for business use.
DAA-GRS-2017-0009-0001 (IT program and capital investment planning records) - Destroy when 7 years old, but 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 statue 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.

5 U.S.C. Section 301 Departmental Regulations. Information required to assist official and employees of the Navy in the management, supervision, and administration of Navy personnel and the operations of related personnel affairs and functions.

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.

OMB package submitted and OMB Control Number 0703-EPWP assigned. The 60-Day Federal Register Notice for 0703-EPWP, "NAVSUP Enterprise Web Portal," was published in the Federal Register on February 10th 2023. The Docket ID is USN-2023-HQ-0007.