PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Personnel Database (NPDB)
Department of the Navy - SPAWAR - PMW 240

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	DITPR ID: 13635 DITPR DON ID: 22136
☐	**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 UII: 007-000003899

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 N01080-1, N01080-2, N01080-3

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:

N01080-1

10 U.S.C. 5013, Secretary of the Navy
DoDI 1336.08, Military Human Resource Records Life Cycle Management
DoDI 1336.05, Automated Extract of Active Duty Military Personnel Records
DoDI 7730.54, Reserve Components Common Personnel Data System (RCCPDS)
Chief of Naval Operations Instructions OPNAVINST 1070.2 Series, Automated Extracts of Active Duty Military Personnel Records
OPNAVINST 1001.19 Series, Reserve Components Common Personnel Data System (RCCPDS)
E.O. 9397 (SSN), as amended.

N01080-2

10 U.S.C. 5013, Secretary of the Navy
E.O. 9397 (SSN), as amended.

N01080-3

5 U.S.C. 301, Department Regulations
E.O. 9397 (SSN), as amended.

Additional authorities:

Authority to Operate (ATO) The Unclassified and Classified Navy Personnel Command (NPC) Defense Enterprise Computing Center (DECC) Mechanicsburg Mainframe Applications on the Legacy Network at Mechanicsburg, PA (FY10L0155) DITPR-DON 20625, 8320, 20634, 10332, 7367, 10332, 7310, 22134, 22136, 7378, 8323 AND 8120 of 25NOV2009

DECC Mechanicsburg Mainframe Assets List of 25NOV2009

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.

NPDB is the Navy's single source database, consolidating Navy Manpower and Personnel data from the Navy's current databases. It contains current and historical data on more than 1.75 million Navy members and annuitants, including officers, candidates, enlisted active and inactive, as well as those in a retired status. The Joint Personnel Adjudication System (JPAS), Active Component Common Personnel Data System (ACCPDS), and Reserve Component Common Personnel Data System (RCCPDS) all rely on NPDB data.

PII data collected: Name, SSN, citizenship, legal status,gender, race/ethnicity, birth date, place of birth, mailing/home address, religious preference, security clearance, spouse information: if spouse is military, SSN and military status information is captured; marital status, military records, education information: college name, level of education, sponsor, service school attended.

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

PII data is stored on the NPDB database on a Department of Defense Mainframe computer. The Defense Enterprise Computing Center (DECC) is responsible for operation of the mainframe. The risk of data disclosure is very low. This system is protected by DON policy-compliant passwords, ACF2 access methods, encryption and firewalls to ensure only authorized personnel gain access to private information. Authorization to access the NPDB database via online screens is the responsibility of the NPDB Database Administrators. Within the computer center, controls have been established to disseminate computer output over the counter only to authorized users. Specific procedures are also in force for the disposal of computer output. Output material in the sensitive category, i.e., inadvertent or unauthorized disclosure that would result in harm, embarrassment, inconvenience or unfairness to the individual, will be shredded. Computer files are kept in a secure, continuously manned area and are accessible only to authorized computer operators, programmers, enlisted management, placement, and distributing personnel who are directed to respond to valid, official request for data. These accesses are controlled and monitored by the security system.

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. NPDB provides data to Navy Manpower, Personnel and Distribution Systems that reside on the same mainframe. NPDB also sends personnel data to EMPRS, NPDB-Web/BOL, Perform To Serve, NTMPS, and OCARS

☒ **Other DoD Components.**

Specify. NPDB provides data to Defense Manpower Data Center(DMDC), JPAS (Joint Personnel Adjudication system.

☒ **Other Federal Agencies.**

Specify. Social Security Administration

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. N65236-13-D-4940 task 0004 [POP is 1-Jul-2015 - 30-Jun-2015, with 2 option years]
AVENTURE TECHNOLOGIES, LLC
2600 PARK TOWER DRIVE, SUITE 1000
VIENNA VA 22180
. The contractor shall ensure all guidelines for the protection of Privacy Act (PA) Data and the safeguarding of Personally Identifiable Information (PII) are followed.
. The contractor shall ensure all technical data rights and source code developed under this task order ultimately becomes property of the government upon completion of the task order.
. Federal Acquisition Regulation (FAR) clauses are documented in the base contract

☐ **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.

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.

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.