PRIVACY IMPACT ASSESSMENT (PIA)

For the

Officer Assignment Information System (OAIS) II
Department of the Navy - SPAWAR - PEO EIS

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: 13645 DITPR DON ID: 7378
☐	**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: 007-000003875

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 N01080-2, M01754-6, N01301-2

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 N01301-2 authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 620, Active duty lists
10 U.S.C. 617, Reports of Selection Boards
E.O. 9397 (SSN) as amended

SORN N01080-2 authorities:

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

SORN M01754-6 authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, U.S. Marine Corps
MCO 1754.4, Exceptional Family Member Program
NAVADMIN 285/11, Exceptional Family Member Program Capability in the Navy Family Accountability and Assessment System

DoD 6025.18-R, DoD Health Information Privacy Regulation
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 Officer Assignment Information System II (OAIS II) provides on-line officer personnel information and Permanent Change of Station (PCS) order writing functions, including separation and retirement orders, for use by officer assignment and placement personnel. System handling information that is important to the support of deployed and contingency forces. The System provides users the capability for rapid, AD-Hoc queries of personnel and activity data in support of distribution processes, manning, and assignments in response to requests from higher authority (BUPERS, CNP, CNO, and DOD).

Personal information collected consist of: Name, Social Security Number (SSN), Citizenship, Gender, Race/ Ethnicity, Birth Date, Military Records and Education Information. The system may also include Religious Preference, Security Clearance, Military Spouse Information, some Medical Information pertaining to Exceptional Family Members.

Employment information: This system no longer collects PII for this category.

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

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 as well as the following controls which are used to mitigate the risks:
a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application.
These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
d) Audits. This includes review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application. Transactions are logged based on user evaluation of the information.
e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements.
Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.
f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.

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. The information is shared with SPAWAR application programmers/analysts

that maintain the system software and system administrators. Information is shared with the Member, his/her, Command (Commanding Officer, Executive Officer, and Administrative Officer), his/her Detailer (placement personnel). The information is also sent to other DON systems by interface for need to know requirements of those systems.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

Contractor name: eVenture Technologies, LLC
Contract Number: N69250-07-D-0300 Task Order 0370 eVenture Technologies, LLC,
52.224 - 1 - Privacy Act Notification
The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

52.224 - 2 - Privacy Act

(a) The Contractor agrees to
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies
(i) The systems of records; and (ii) The design, development, or operation work that the contractor is to perform;
(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act;
(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.

(c) For Systems of Record,
(1) Operation of a system of records, as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
(2) Record, as used in this clause, means any item, collection, or grouping of

information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) System of records on individuals, as used in this clause means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

☐ **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.