PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Enlisted System (NES)
Department of the Navy - SPAWAR - PEO EIS 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: 13431 DITPR DON ID: 22134
☐	**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: 007-000003898

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

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 N01080-1 authorities:

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

Other authorities:

DoDI 1336.05, Automated Extract of Active Duty Military Personnel Records

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 Navy Enlisted System (NES) is the Navy's corporate database of authoritative data on all active duty Navy enlisted personnel. The system generates and maintains the official automated personnel records of all United States Navy (USN) active duty enlisted personnel for both current and historical purposes. NES is primarily used to calculate enlisted strength, to authorize the establishment of a pay record at Defense Finance Accounting Service, and to prepare Enlisted Distribution Verification Reports (EDVR) for distribution to field activities. The enlisted distribution and promotion processes are dependent upon the quality of NES information, as are numerous managerial and Congressional groups overseeing aggregated information about the active enlisted population.

PII data collected: Name, SSN, citizenship, legal status, gender, race/ethnicity, birth date, birth place, security clearance, spouse information: If the spouse is in the military, SSN and branch of service is collected; marital status, child information: location of child, if on base, and special needs information; military records: unique identification code (UIC), afloat or ashore, promotion info, rates, evaluations, promotions, and demotions; education information: Highest Degree level, Degree type and military education. School name is not collected; and religious preference.

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

PII data is stored in NES on the Enlisted Master File (EMF). The EMF is stored on a Department of Defense Mainframe computer. The Defense Enterprise Computing Center (DECC) is responsible for operation of the mainframe.

This system is protected by DON policy-compliant passwords, ACF2 access methods, encryption and fire walls to ensure only authorized personnel gain access to private information. Transmission of display data sent to and from the mainframe is encrypted.

NES exchanges data with Navy Military Personnel Distribution Systems, Navy Reserve Personnel Systems, and Navy Manpower Systems, which reside on the same mainframe region. NES also sends and receives personnel data from the Navy Training and Education Systems, and the Navy Standard Integrated Personnel System (NSIPS). Data flows through DoN system to DoN system through secure channels. Authorization to access NES data is the responsibility of the Navy Personnel Command (NPC), currently PERS341.

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. Navy Bureau Of Medicine and Surgery (BUMED), Chief of Naval Education and Training (CNET), Navy Manpower, Personnel, and Distribution Systems.

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC), Defense Finance Accounting Service (DFAS)

☒ **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.

Contractor name: eVenture Technologies, LLC
Contract Number: N69250-07-D-0300 Task Order 0308 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; and
(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 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 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 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.