PRIVACY IMPACT ASSESSMENT (PIA)

For the

<table>
<thead>
<tr>
<th>E-Submission (ESUB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of the Navy - BUPERS</td>
</tr>
</tbody>
</table>

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 DADMS ID 95358
☐ 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

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 N01070-3

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
No PII is collected directly from the individual.

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 Navy Military Personnel Records System (April 15, 2010, 75 FR 19627) authorities:

10 U.S.C. 5013, Secretary of the Navy
42 U.S.C. 10606 as implemented by DoD Instruction 1030.1
Victim and Witness Assistance Procedures
E.O. 9397 (SSN), as amended.

Other authorities:

DODI 1336.08. Military Human Resource Records Life Cycle Management
BUPERSINST 1070.27C Document Submission Guidelines for Electronic Military Personnel Records System

DD FORM 2930 NOV 2008 Page 3 of 17
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.

E-Submission (ESUB) is an Electronic Military Personnel Records System (EMPRS) application hosted on BOL with access controlled through the SAAR-N process. This application allows select personnel, such as Personnel Specialists within Personnel Support Detachments and Personnel Offices, to electronically submit files to be included in service members' Official Military Personnel Files maintained in the EMPRS. E-Sub collects the SSN entered into the application as reflected on each document to be submitted (masking the SSN in the e-Sub application), queries corporate data to match the SSN to a member's name for an OMPF record contained in EMPRS. If a record is found, e-Sub allows the Personnel Specialist to upload an image of a service record document containing a member's name and SSN into EMPRS.

Personal information collected: Name, SSN, Citizenship, Legal Status, Gender, Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Phone Number, Home Telephone Number, Mailing/Home Address, Religious Preference, Spouse and Child Information, Marital Status, and Other: Unit Identification Code (UIC).

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

The risks are small compared to mailing of documents and the risk of losing a package in route.

The SSN as entered in the e-Sub application is masked during typing; inadvertent exposure of PII as a result of user mistake is mitigated by restricting access to the application and multiple layers of quality control to preclude misfiled documents.

Attacks or intrusion into BOL by unauthorized personnel; mitigated through the use of PKI, firewall, restricted access to files based on user permissions.

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 Personnel Offices submitting the documents and Navy Personnel Command employees receiving the documents.

☐ 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. Lockheed Martin: Personnel working on this contract may be required to handle information that is covered by the Privacy Act of 1974 (Title 5 of the U.S. Code, Section 552.a). Contractors working directly with Military Personnel Records will be
required to sign a Non-disclosure agreement. The requirement to control access to sensitive information applies to all US government IT systems and/or areas where unclassified but sensitive information may be discussed, displayed or maintained. DON policy prescribes that all unclassified data that has not been approved for public release and is stored on mobile computing devices must be treated as sensitive data and encrypted using commercially available encryption technology. Whenever granted access to sensitive information, contractor employees shall follow applicable DOD/DON instructions, regulations, policies and procedures when reviewing, processing, producing, protecting, destroying and/or storing that information. Operational Security (OPSEC) procedures and practices must be implemented by both the contractor and contract employee to protect the product, information, services, operations and missions related to the contract. The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the Navy Command's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer.

National Sourcing Inc.: The contractor shall ensure that employees assigned to this contract, understand and adhere to the Privacy Act of 1974. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations. The contractor is responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/privileged information which may involve the contractor or the contractor's personnel or to which they may have access may subject the contractor and/or the contractor's employees to criminal liability under Title 18, section 793 and 798 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. All programs and materials developed at government expense during the course of this contract are the property of the government.

Contract contains FAR Privacy Clauses.

☐ 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.

No PII is 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.

No PII is 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  ☒ None

Describe each applicable format.

No PII is 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.