



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Advancement/Selection Board Application (ADV/SEL Board)

Department of the Navy - BUPERS

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

**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
- 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

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**

ADV/SEL Board does not collect PII from members of the public.

**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 Enlisted Master File Automated Systems (June 07, 2013, 78 FR 34354) authorities:

10 U.S.C. 5013, Secretary of the Navy; Department of Defense Instructions 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; and OPNAVINST 1001.19 Series, Reserve Components Common Personnel Data System (RCCPDS); and E.O. 9397 (SSN), as amended.

SORN N01080-2 Officer Master File Automated Systems (November 01, 2013, 78 FR 65620) authorities:

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

SORN N01080-3 Reserve Command Management Information (February 22, 1993, 58 FR 10706) authorities:

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

Other authorities:

1. Title 10

2. BUPERSINST 1430.16(series), ADVANCEMENT MANUAL FOR ENLISTED PERSONNEL OF THE U.S. NAVY AND U. S. NAVY RESERVE

**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.

Advancement/Selection Board Application is a BUPERS Online (BOL) that provides a platform for Navy Personnel Command, Career Progression (PERS 8), Naval Education Training Professional Development Technology Center (NETPDC) N321, and Navy Recruiting Command (NRC) to load/post promotion, selection, continuation board, and eligibility results for command and individual access. The information applies to United States Navy (USN) personnel under the purview of the Navy Personnel Command (NPC), Millington, Tennessee. Web-based BOL Advancement/Selection and Continuation Board Application. It will capture the requirements as it applies to promotion, selection, continuation board, and eligibility results posting and access. It will not be utilized to increase or enhance functionality. Web-based BOL Advancement/Selection and Continuation Board Application. It will capture the requirements as it applies to promotion, selection.

Personal information collected: Name, SSN, DoD ID number, promotion/advancement results.

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

The risks associated with maintaining PII in this application are potential compromise by a disgruntled employ or hacking. Except for internal malicious activity, mitigations are provided by the security controls provided by BOL and per DoD and DON policy. All PII stored on shared drives is protected by ensuring all folders are secured with security groups. These security groups are updated as soon as an employee departs the command. The SSN is never displayed on the screen, it is only used in the 'background' to ensure the correct person is identified.

**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 Command (NPC) PERS-54, and PERS-3, Naval Education and Training Professional Development Center (NETPDC) and Navy Recruiting Command (NRC)

**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.

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.

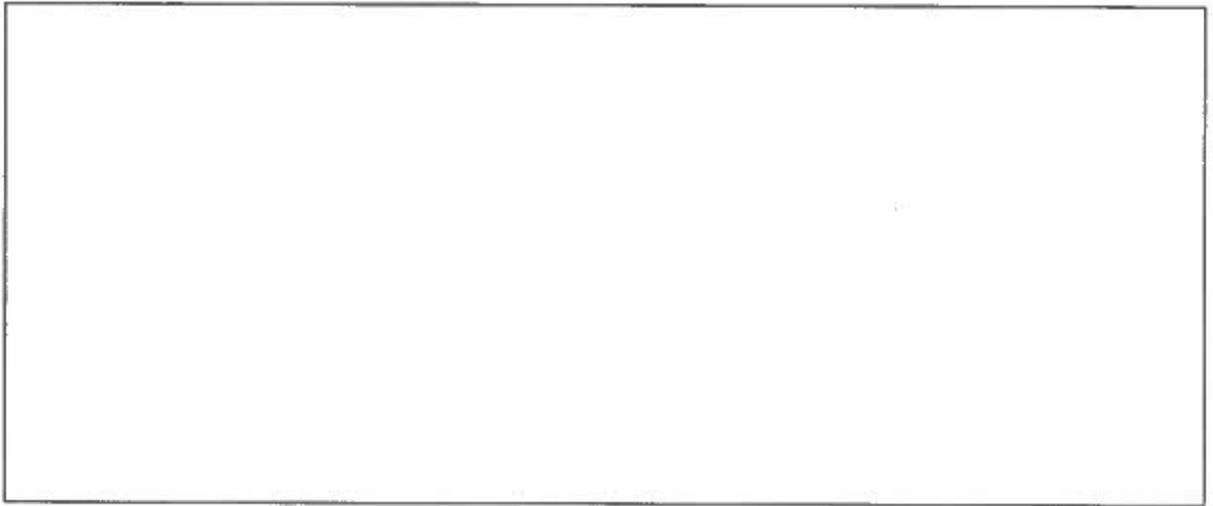
PII is not collected from the individual.

**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.**