PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Accessions Security Information System (NASIS)
Department of the Navy - BUPERS - NRC

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: 15574 DITPR DON: 22563
☐	**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: 007-000004865

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 N01133-2; N01131-1 SORNS are being replaced by N01130-1(At

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 0703-0062

Enter Expiration Date 04-30-2018

☐ **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 N01131-1, Officer Selection and Appointment System (June 14, 2006, 71 FR 34328)

5 U.S.C. 301, Departmental Regulations, 10 U.S.C. Sections governing authority to appoint officers; 10 U.S.C. 591, 600, 716, 2107, 2122, 5579, 5600; Merchant Marine Act of 1939 (as amended); and E.O.s 9397 (SSN), as amended, 10450, and 11652.

SORN N01133-2, Recruiting Enlisted Selection System (April 01, 2008, 73 FR 17336)

10 U.S.C. 133, 275, 503, 504, 508, 510, 672, 1071-1087, 1168, 1169, 1475-1480, 1553, 5013; and 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 NAVY ACCESSIONS SECURITY INFORMATION SYSTEM (NASIS) collects data from future sailors to initiate a personal security investigations for all officer, enlisted, active and reserve Navy personnel. The information for security clearance investigation is submitted to the Joint Personnel Adjudication System (JPAS) to initiate an investigation. All future sailors must complete the SF86 request for security clearance and are required to have an open investigation prior to shipping to boot-camp. NASIS is Navy's security clearance data collection tool and interfaces with JPAS. Background: All accessions services were required by Office of Personnel Management (OPM) to develop their own data collection tool for security clearance request information because of the sheer number of submissions generated from recruiting commands annually. NASIS provides functionality not inherent in eQIP and JPAS. Recruiting commands are not authorized to submit security clearance information directly into eQIP. The NASIS functionality will be subsumed by PRIDE MOD in FY17.

PII Collected: Name, Other Names Used, SSN, Driver's License, DoD ID Number, Citizenship, Legal Status, Gender, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Personal Email Address, mailing/Home Address, Security Clearance, Mother's Maiden Name, Mother's Middle Name, Spouse Information, Marital Status, Child Information, Financial Information, Medical Information, Law Enforcement Information, Employment Information, Military Records, Education Information.

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g. fire, flood, etc...)

The following controls 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. Access is accomplished through a mixture of cryptographic logon (PKE) and public key certificate (PKI). Users logging on locally must present a cryptographic token in the form of a DoD CAC in conjunction with a PIN for identification and authentication. Remote logon for administrator functions requires an alternate cryptographic token specifically for that purpose. Web server access for Navy personnel requires presentation of a DoD PKI certificate to negotiate an SSL-enabled session.

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 or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.

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. Navy Recruiting Command

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Joint Personnel Adjudication System (JPAS) application maintained by Defense Manpower Data Center (DMDC) and Electronic Questionnaires for Investigations Processing (e-QIP) web application maintained by OPM.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

During applicant interviews with recruiters, applicants are informed of the purpose for gathering the personal information and of the protection afforded them under the Privacy Act of 1974. At this point, they can object to the collection, and the recruitment process will end.

(2) If "No," state the reason why individuals cannot object.

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.

Consent is provided by the individual's signing of the Privacy Act Statement of 1974 at the beginning of the recruiting and accessions process. All information collected from individuals is required for processing the applicant into the Navy. At this point, they can not sign and the recruitment process will end.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.	Required Privacy Act disclaimer is displayed throughout the NRC application. The DoD required Privacy and Monitoring Advisory is available at login. Applicants are also required to read and sign the Privacy Act Statement on the DD Form 1966/1, Record of Military Processing - Armed Forces of the United States.

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.