PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personalized Recruiting for Immediate and Delayed Enlistment Modernization (PRIDE MOD)
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 DON ID: 21958 DITPR ID: 9728
☐	**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: 007-000003493

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 N01131-1, N01133-1, and N01133-2

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	Only collection is for SF-86 which has an OMB Control number of 3206 0005
Enter Expiration Date	No expiration date provided, although the

☐ **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 Authorities:

N01131-1

55 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)
E.O. 9397, as amended, 10450, and 11652.

N01133-1

55 U.S.C. 301 and 302, Departmental Regulations
4 U.S.C. 3101, 3702
E.O. 9397, as amended.

N01133-2

10 U.S.C. 133, 275, 503, 504, 508, 510, 672, 1071-1087, 1168, 1169, 1475-1480, 1553, 5013
E.O. 9397, as amended.

Other authorities:

Primary Directives implementing above statues:

Navy Recruiting Manual - Enlisted, COMNAVCRUITCOMINST 1130.8J
Navy Recruiting Manual - Officer, COMNAVCRUITCOMINST 1131.2E

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.

PRIDE MOD supports the Navy Recruiting Command's officer and enlisted, active and reserve accessions process providing applicants designation, classification and allocation of training resources. PRIDE MOD captures officer and enlisted applicant qualifications data, e.g. aptitude, test scores, education, color perception, etc. and determines what officer designator, enlisted ratings, and other programs an applicant is qualified for. PRIDE MOD is also used to process incentives, waivers as required, and make Class A school reservations.

The functional owner of PRIDE MOD is Commander, Navy Recruiting Command. PRIDE MOD is a web services application hosted at the SPAWAR Atlantic Data Center, New Orleans, LA. NOLA provides system backup, recovery, and fail-over services.

Personal information includes: name, SSN, truncated SSN, driver's license number, other ID numbers, citizenship, legal status, gender, race/ethnicity, date of birth, place of birth, personal cell phone number, home telephone number, personal email address, home address,religious preference, security clearance, mother's maiden name, mother's middle name, spouse information: Name, current address,Birth Date, Social Security Number (SSN), phone number and place of employment; marital status, child information: Name, current address, Birth Date, SSN; financial information: Past and Present income and debt. Current status of all accounts; medical information: Past and Present records of medical conditions and treatment; disability information: Documentation of the reason and status of any disability determinations; law enforcement information: Records checks on all past law violations; employment information: Past and Present Employer's names, addresses and contact information. The periods of employment for each employer; military records, emergency contact information, education information: Name, address and phone number of all institutions education was obtained and the time periods of attendance. Transcripts from the listed institutions; digital photograph, and biometric fingerprints.

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

Risks:

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

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that PRIDE MOD, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

Since PRIDE MOD operates on the NMCI Network, there is a risk that security controls could be disabled for

maintenance and other purposes. The risk would be that the security controls would not be reset.

All systems are vulnerable to "insider threats". PRIDE Mod II managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to PRIDE Mod II. These individuals have gone through extensive background and employment investigations.

Mitigations:

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 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 (NRC), Navy Personnel Command (NPC)

☒ **Other DoD Components.**

Specify. Military Entrance Processing Command (MEPCOM)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. CGI Federal

Contract # N00039-13-D-0001, Task Orders 02 and 03

5.2.12.3 Data Protection

The Contractor shall comply with the DON Privacy program per SECNAVINST 5211.5E.

The Contractor shall ensure all categories of sensitive information, including Personally Identifiable Information (PII), are secured and in compliance with all IA Controls from the DoDI 8500.2, specifically IA Controls DCFA-1 and DCSR-2. Compliance includes the encryption of "data in transit" and "data at rest" as required by the data owner.

The Contractor shall comply with DON CIO MSG DTG 171952Z APR 07 to ensure that all PII is properly safeguarded. The requirement under the E-Government Act of 2002, mandates that all PII be protected. In addition, systems processing PII must have completed a Privacy Impact Assessment (PIA) and register that PIA with DON CIO.

The Contractor shall provide controlled access to prevent unauthorized access to DoD systems and information using identification and authentication as well as encryption.

☐ **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.

The only information collected from the pubic from this system is that information used to populate the SF-86. Applicants are informed of the purpose for gathering this 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 at the beginning of the application process. If the applicant chooses not to sign this form, the recruitment process will end.

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

N/a.

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.

Applicants are required to read and sign (with biometric fingerprint) 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.