PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Web Recruiting Tools (WebRTools)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

03/05/19

U.S. Navy - Bureau of Naval Personnel (BUPERS) / Navy Recruiting Command (NRC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

WEB RECRUITING TOOLS (WEBRTOOLS) supports the Navy Recruiting Command by providing contact management capabilities for Active and Reserve Enlisted and Officer recruiting. It is a Web-enabled application which provides applicant lead and contact information for over 4000 field Recruiters.WebRTools. Through a series of on-line processes, WebRTools provides recruiters with the ability to track leads and manage their recruiting contacts. The application provides the capability to input information on applicants to include personal data, remarks, and information relating to contact with the individuals. WebRTools provides a Sales Activity Analysis capability to determine effectiveness of recruiting in specific areas. WebRTools serves as the single primary contact management system for Active and Reserve, Enlisted and Officer Recruiting providing leads information and tracking progress of contact management. As leads are received from they are processed immediately and the data is available to the appropriate recruiter. WebRTools is the primary source of applicant data for the PRIDE Mod system. WebRTools Self Service for Applicants (WRT SSA) system is an Applicant tool to be utilized by personnel applying to join the Navy through the Internet from the convenience of their homes or offices. In addition, the system will be a key Information Delivery System (IDS) providing Navy Recruiters with near real-time awareness of hot Leads. WebRtools MepsTrack provides the recruiter the ability to track his applicant through the MEPS process, displaying the times the applicant completes each step of his process.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The data is collected to verify and validate applicant's eligibility for accession into the US Navy. The information is also used to determine applicant eligibility for and qualification for specific Navy programs and jobs.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

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

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

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.

g. **When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided.** *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

Required Privacy Act disclaimer is displayed throughout the NRC system. 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.

h. **With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?** *(Check all that apply)*

[X] Within the DoD Component	Specify.	Navy Recruiting Command
[ ] Other DoD Components	Specify.	
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	
[ ] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
[ ] Other *(e.g., commercial providers, colleges).*	Specify.	

i. **Source of the PII collected is:** *(Check all that apply and list all information systems if applicable)*

[X] Individuals
[X] Existing DoD Information Systems
[X] Other Federal Information Systems
[ ] Databases
[ ] Commercial Systems

There are numerous sources of the PII collected which include Individual, Law Enforcement agencies, Social Security Administration, schools attended, colleges attended, employers, medical information Department of Vital Statistics.

j. **How will the information be collected?** *(Check all that apply and list all Official Form Numbers if applicable)*

[X] E-mail
[X] Face-to-Face Contact
[X] Fax
[X] Information Sharing - System to System
[ ] Other *(If Other, enter the information in the box below)*
[ ] Official Form (*Enter Form Number(s) in the box below*)
[X] Paper
[X] Telephone Interview
[X] Website/E-Form

k. **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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier N01131-1, N01133-2, N01130-1(Conso

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. **What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?**

(1) NARA Job Number or General Records Schedule Authority. DAA-NU-2015-0001-0[illegible]

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

These records are scheduled under SSIC 1000-29 and are TEMPORARY. Cutoff at CY. Destroy when 5 years old. Information is stored in an encrypted state and is backed up regularly.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN N01130-1 is a consolidation of the below outdated SORNs and has been in the approval process for an extended period. Once approved, all of the below laws and regulations will be covered under one SORN.

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.

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, 10450, and 11652.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Awaiting OMB 0703-0062 and OMB 0703-0029 approval before submission of further OMB requests for NRC systems. Process to renew OMB is currently with DNS 36 for final signature.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☒ Birth Date	☒ Child Information
☒ Citizenship	☒ Disability Information	☐ DoD ID Number
☒ Driver's License	☒ Education Information	☒ Emergency Contact
☒ Employment Information	☒ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☒ Law Enforcement Information	☒ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☒ Medical Information
☒ Military Records	☒ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☒ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☒ Race/Ethnicity	☒ Rank/Grade	☒ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

-Name: First, Middle and Last
-Birth Date: Month Day and Year
-Medical Information: DD Forms 2807, 2808 and other general medical information used to determine medical waivers for accession to the Navy.
-Social Security Number (SSN): 9 digits
-Gender: M/F
- Spouse Information: Name, current address,Birth Date, Social Security Number (SSN), phone number and place of employment.
- 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 information 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.
- Education Information: Name, address and phone number of all institutions education was obtained and the time periods of attendance. Transcripts from the listed institutions.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Gary C. Peterson, NRC Deputy Commander - 7/7/2017.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Computer Matching; Law Enforcement, National Security and Credentialing.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

SSN use is still required. Navy would be unable to execute its active enlisted mission. This could result in fraudulent enlistments which would drive recruiting and training costs. In addition, until the enlistment documents are revised, it would require manual input to recruiting documents and the DD Form 4 enlistment contract. Applicants do not have a DoD ID as they are not issued their common access card (CAC) until they arrive at boot camp so it is impossible to assess them using a DoD ID.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

Explained above in question 3.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☒ Cipher Locks
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☒ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☐ If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☐ If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

☐ Biometrics	☒ Command Access Card (CAC)	☒ DoD Public Key Infrastructure Certificates
☒ Encryption of Data at Rest	☒ Encryption of Data in Transit	☐ External Certificate Authority Certificates
☒ Firewall	☒ Intrusion Detection System (IDS)	☒ Least Privilege Access
☒ Role-Based Access Controls	☐ Used Only for Privileged (Elevated Roles)	☒ User Identification and Password
☒ Virtual Private Network (VPN)	☐ If Other, enter the information in the box below	

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Access Controls: Access controls limit access to the application and/or specific functional areas of the all applications. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Confidentiality: Confidentiality ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity: Integrity ensures that data has not been altered or destroyed in an unauthorized manner. Audits: Audits to review and examine records, activities, and system parameters, to assess the adequacy of maintaining, managing, and controlling events that may degrade the security posture of the all applications. Training: Security training is provided on a continuous basis to keep users alert to the security requirements. Physical Security: Physical security consists of placing servers that contain privileged information in a secure and protected location, to limit access to this location to individuals who would have a need to access the servers. Access to each application is limited to authorized and appropriately cleared personnel as determined by the system manager. Physical entry is restricted by use of locks, guards, and is accessible only to authorized, cleared personnel.