



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Reserve Forces Manpower Tools (RFMT)  
(Revised 20161116 to add collection of DoD ID Number (EDIPI) and update the UII)

Department of the Navy - CNRFC

### **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**

**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 Authorities:

5 U.S.C. 301, Department Regulations;  
DoD 6025.18-R, DoD Health Information Privacy Regulation;  
and E.O. 9397 (SSN), as amended

Other Authorities:

10 U.S.C. 5013, Department of the Navy  
10 U.S.C. Subtitle E, Reserve Components  
1007, Administration of Reserve Components  
BUPERS Instruction 1001.39F, Administration Procedures for Navy Personnel  
OPNAV Instruction 100.16K, Navy Total Force Manpower Policies and Procedures

**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.

RFMT, formally known as APPLY-SLATER, is a system comprised of a web accessible database and a suite of interoperable, personnel-related modules that support the mission of NAVRESFOR. These modules are APPLY, SLATER and Inactive Duty Training Order Writer (IDTOW). Each module has a specific set of capabilities; however, the data flow for a Reservist's assignment can be traced from APPLY (where the Reservists "APPLY" to billets), to SLATER (where Operational Support Officers/Boards "SLATE" Reservists to billets), to IDTOW (where the official Inactive Duty Training (IDT) Orders are generated and released to the Reservist).

RFMT users connect to the system during the allotted period during the fiscal year in order to upload their applications for billets. Once identification is made, the member can see all available billets they are qualified to apply for, as set by the ESC. The member identifies their selections and then sets a priority corresponding to their desire for the billet. Member personal information, such as address, email, duty history, etc. may be updated via the RFMT process. APPLY allows a centralized means of identifying, advertising, and filling of junior and senior command and non-command billets across the Reserve community and allows community leaders to set filter criteria restricting selection to community standards. Once the application period is complete the RFMT website is shut down for the slating "SLATER" selection process. The slating process is used by the Navy Reserve National Command and Senior Officer (05/06) Non-Command Billet Screening and Assignment RFMT Board members to ultimately assign billets to the most qualified officer. This configuration involves the SLATER server and four laptop computers in a closed room. Upon completion of the board process, the RFMT website is re-opened and results are made available to all applicants. Applicants then elect to accept or decline assigned orders. If accepted, RFMT generates orders for further processing in IDTOW.

PII collected includes: Name, SSN, DoD ID Number (EDIPI), Citizenship, Gender, Race/Ethnicity, Birth Date, Home Telephone Number, Mailing/Home Address, Security Clearance, Marital Status, Military Records, and Education Information: education level/major/speciality code, high school diploma or GED and years of education.

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

The disclosure of the information stored in the RFMT could lead to identity theft/fraud or perhaps be used to target individuals for exploitation. The risks are mitigated via application security controls for user login, two-factor authentication via common access card (CAC), system monitoring by system administrators, policies and system security controls as outlined in the certification and accreditation (C&A) plan.

The data stored in the RFMT is protected by a variety of methods including data-at-rest/data-in-transit encryption, firewalls and intrusion detection systems (IDSs). Access to the data is restricted to authorized users only. All system users are required to undergo annual Privacy Act and Information Assurance (IA) training.

**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.

**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.

CACI, Inc.

The contractor shall have an operational security program in strict compliance with the National Industrial Security Program Operating Manual (Department of Defense (DoD) 5220.22-M) and Space and Naval Warfare Systems Center, Atlantic (SSCA) security directives at the time of award. Clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted.

If contractor personnel require access to any Navy IT systems or resources at SSCA (directly or indirectly), all contractor personnel shall be required to complete the mandatory annual IA training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified Contracting Officer's Representative (COR).

The contractor shall demonstrate expertise in supporting and complying with DoN and DoD enterprise initiatives that include Personally Identifiable Information (PII).

The Contractor shall conform to the provisions of DOD 5220.22M, SECNAVINST 5510.30, and the Privacy Act of 1974.

Contractor personnel shall sign a Non-Disclosure Agreement when tasking requires access to PII.

**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 solicited from the individual by RFMT. PII is collected by the authoritative source systems and

securely transferred to RFMT on a periodic basis.

**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.

The individual's opportunity to consent would be at the collection point by the authoritative source systems. RFMT stores PII, but does not provide any mechanism for the collection of PII 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.

Serving as the National Command and Senior Non-Command Billet Screening and Assignment, RFMT stores data it receives via system to system interfaces with the various authoritative source systems. Individuals are never asked to provide PII to RFMT. The PII data contained in RFMT is supplied by authoritative source systems. The authoritative source systems collecting the PII has the responsibility of providing the individual with any information related to the collection of PII.



**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.**