



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Reserve Integrated Management System (Financial Management) / RIMS (FM)

Department of the Navy - SPAWAR - PEO EIS - PMW 240

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

DITPR ID: 44	DITPR-DON ID: 8109
--------------	--------------------
- 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: 007-000001645

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

N01571-1

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, Departmental Regulations;
10 U.S.C. 5013, Secretary of the Navy;
COMNAVRES Instruction 1571.1D, Ordering Processing and Transportation Arrangements for Navy Reservists;
E.O. 9397 (SSN).

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.

Reserve Integrated Management System (RIMS) Financial Management (FM) is a mission critical Financial Management application created to manage those funds appropriated by Congress to the Navy Reserves.

RIMS (FM) writes, modifies and cancels orders for Naval Reservists performing ACDUTRA; to issue seabags, death benefits paid, per diem, travel, subsistence, drill pay, ACDUTRA and Temporary Active Duty (TEMAC) pay, disability payments, bonuses, school costs and special pay such as flight and sea pay, and to monitor training needs.

System comprises records reflecting information pertaining to reservist's Active Duty for Training (ACDUTRA). The system also contains a Standard Document Number (SDN) which is used to track cost of training, clothing and subsistence that is provided to the reservist.

Operational Relevance: 1) Manages RPN Funds for AT, ADT, IDTT 2) Manages Reimbursable Work Orders 3) Post Obligations to STARS-FL 4) Receives Bonus information from RHS, formats and posts to STARS-FL.

PII collected: Name, Social Security Number (SSN), Rank/Grade, and Financial Information: Funding Source Code (FSC) and Standard Document Number mapped to FSC.

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

Potential threats/risks that may impact the integrity, availability, and confidentiality of the RIMS(FM) system includes individual users mishandling of data and firewall issues. Mitigations include: DoD PKI certificates are used for server and client authentication. Logins to the web page are controlled by the application. User authentication and role-based authorization are implemented to grant access to RIMS(FM). All external communications to the web server are protected by an external firewall, host address block / allow lists and HyperText Transfer Protocol (HTTP) of Secure Sockets Layer (SSL) encryption. An outer firewall interface will require HTTP of SSL opened inbound to the web servers. System logins are limited, in general, to administrators and developers. The RIMS(FM) production database server resides within the Data Center's Production Private Access Zone of the EDMZ - providing another level of security.

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.

N65236-13-D-4940 task 0004 [POP is 1-Jul-2015 - 30-Jun-2015, with 2 option years]
AVENTURE TECHNOLOGIES, LLC
2600 PARK TOWER DRIVE, SUITE 1000
VIENNA VA 22180
The contractor shall ensure all guidelines for the protection of Privacy Act (PA) Data and the safeguarding of Personally Identifiable Information (PII) are followed.
The contractor shall ensure all technical data rights and source code developed under this task order ultimately becomes property of the government upon completion of the task order.
Federal Acquisition Regulation (FAR) clauses are documented in the base contract.

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.

PII is not collected directly from the individual.

(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.

PII is not collected directly from the individual.

[Empty rectangular box]

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

PII is not collected directly 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 directly 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.