



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Reserve Headquarters Support (RHS)

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
- 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 N01080-3 authorities:

5 U.S.C. 301, Department Regulations and 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.

RHS is a COMNAVRESFORCOM mission-critical system used in the data collection and dissemination process for command and control of SELRES Mobilization. RHS supports the Navy Reserve functional areas of manpower, personnel, billet and unit management, mobilization management, and personnel pay management.

RHS provides mission-critical support in the following areas: Reserve Activity Establishment/Disestablishment, Reserve Billet Establishment, Bonus Pay Establishment and Management, Retirement Point Processing, Incentive/Special Pay Management, Inactive Duty Training reporting/processing.

Personal information collected: Name, Social Security Number (SSN), DoD ID Number, Citizenship, Gender, Race/Ethnicity, Birth Date, Home Telephone Number, Mailing/Home Address, Security Clearance, Spouse Information: Name, DOB, and Age; Marital Status, Child Information: Name, DOB, Age, Number of children; Financial Information: Bank Name, Type of Accounts, and Routing Number; Employment Information: Work History and Resume; and Education Information: Level of Education completed, Names of Schools attended, Type of Degree, and Transcripts.

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

Potential threats/risk that may impact the integrity, availability and confidentiality of the RHS system include hardware/software failure, and fire wall issues. These risks are mitigated through the use of DoD PKI certificates for server and client authentication. User authentication and role-based authorization are implemented to grant access to RHS. All external communications to the server are protected by an external firewall, host address block / allow lists and HTTP over SSL encryption. An outer firewall interface will require HTTP over SSL opened inbound to the servers. System logins are limited, in general, to administrators and developers. The production database server resides within the Production Private Access Zone of the EDMZ.

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

Since RHS 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". RHS 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 RHS. These individuals have gone through extensive background and employment investigations. The RHS servers reside within EDMZ hosted by the NMCI.

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.

U.S. Navy - Navy Personnel Command (NPC) and Commander Navy Reserve Force (CNRFC) with a need to know. Career Management System/ Interactive Detailing (CMS/ID), Navy Standard Integrated Personnel System

(NSIPS), Navy Personnel Data Base (NPDB), Navy Personnel Data Base (CeTARS), Medical Readiness Reporting System (MRRS), Navy-Marine Corps Mobilization Processing System (NMCMPMS), Navy Training Management and Planning System (NTMPS), Navy Reserve Data Warehouse (NRDW), Navy Reserve Order Writing System (NROWS), Reserve Integrated Management System (RIMS) Financial Module (FM), Inactive Manpower and Personnel Management Information System (IMAPMIS)

Other DoD Components.

Specify. Defense Finance and Accounting Service (DJMS-RC) and Department of Defense Military Health System (DMHRSi)

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify. Contract N65236-13-D-4040 Task Order 0004 aVenture Technologies, LLC, Statement of Work stipulates:
- Section 6.1.7: "Ensure all guidelines for the protection of Privacy Act (PA) Data and the safeguarding of Personally Identifiable Information (PII) are followed."
- Section 4.0: In addition to contract clauses C-5 and H-19, requirements, Information assurance and contractor personnel access to SPAWAR LANT New Orleans facilities and DoD information systems will be determined in accordance with the following directives: DoD Directive 8500.1 (Information Assurance) DoD Directive 8500.2 (Information Assurance Implementation) DoD Directive 5200.1 (DoD Information Security Program) DoD Directive 5200.2 (DoD Personnel Security Program) DoD Directive 5200.2-R (DoD Personnel Security Program) SECNAV M-5510.30 (Navy Personnel Security Manual).

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 collected from the individual.

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.

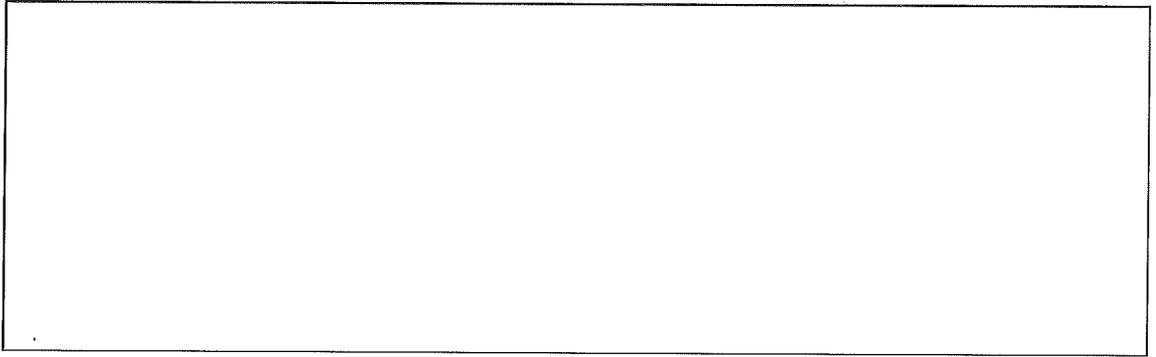
PII is not collected from the individual.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

PII is not collected 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.