



PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

Military Personnel System (MILPERS)

DoD Component Name:

U. S. Navy, Echelon III

SPAWAR Service Center Pacific (SSC Pacific)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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) 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
- 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 Enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

- No

d. Does the DoD information system or electronic collection have 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 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.

- No

e. Does this DoD information system or electronic collection have an 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.

Yes

Enter OMB Control Number

Enter Expiration Date

No

It has been determined that an OMB Control Number is required and the process to obtain one has been initiated. The PIA will be updated accordingly at a later date.

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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.

10 U.S.C. Title 5013, Secretary of the Navy; and Executive Order (EO) 9373 (SSN).
In addition, SPAWAR Systems Command (SPAWARSYSCOM) and SSC Pacific are designated as "Restricted" activities. SECNAVINST 5510.30A, SECNAVINST 5510.36, OPNAVINST 5510.1 (series) and OPNAVINST 5530.14 (series) require a government facility that has been designated as "Restricted" to only admit persons whose duties require access and have been granted appropriate authorization.

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.

The MILPERS application provides the means to track and report information about military personnel assigned to SSC Pacific and SPAWARSSYSCOM. At a basic level it provides military rosters and onboard counts for officers and enlisted personnel. More importantly, it is a tool that identifies skills and experiences that enables the matching of military personnel to active Research and Development (R&D) project staffing requirements and the tracking of organizational assignments. The system is integrated with SSC Pacific's Security Control System (SCS) application, which controls badging and base access. Upon report to this command, the service member's personnel record becomes active in MILPERS and is accessible to SCS for badging.

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

Privacy act data must be accessible only to authorized personnel with a "need-to-know." As a function of providing access to the corporate data, the possibility of a threat by malicious intent is created.

The Corporate Database (CDB) operating environment utilizes the security protection provided at the SSC Pacific Information Systems Computer Operations Facility (ISCOF) combined with the CDB system security design as a response to recognized threats.

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

SPAWARSSYSCOM and SSC Pacific

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

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 the method by which individuals can object to the collection of PII.

Disclosure is voluntary. However, failure to provide the info may result in denial of entry to SPAWAR System Command and SSC Pacific facilities/spaces, as both are designated as "Restricted" activities.

(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.

Disclosure is voluntary. However, failure to provide the info may result in denial of entry to SPAWAR System Command and SSC Pacific facilities/spaces, as both are designated as "Restricted" activities.

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

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.

A Privacy Act Statement and/or a Privacy Advisory are provided prior to collection of PII 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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply in the table below.

<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Other Names Used	<input checked="" type="checkbox"/> Social Security Number (SSN)
<input type="checkbox"/> Truncated SSN	<input type="checkbox"/> Driver's License	<input type="checkbox"/> Other ID Number
<input checked="" type="checkbox"/> Citizenship	<input type="checkbox"/> Legal Status	<input type="checkbox"/> Gender
<input type="checkbox"/> Race/Ethnicity	<input checked="" type="checkbox"/> Birth Date	<input checked="" type="checkbox"/> Place of Birth
<input type="checkbox"/> Personal Cell Telephone Number	<input checked="" type="checkbox"/> Home Telephone Number	<input type="checkbox"/> Personal Email Address
<input checked="" type="checkbox"/> Mailing/Home Address	<input type="checkbox"/> Religious Preference	<input checked="" type="checkbox"/> Security Clearance
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Mother's Middle Name	<input type="checkbox"/> Spouse Information
<input type="checkbox"/> Marital Status	<input type="checkbox"/> Biometrics	<input type="checkbox"/> Child Information
<input type="checkbox"/> Financial Information	<input type="checkbox"/> Medical Information	<input type="checkbox"/> Disability Information
<input type="checkbox"/> Law Enforcement Information	<input checked="" type="checkbox"/> Employment Information	<input checked="" type="checkbox"/> Military Records
<input type="checkbox"/> Emergency Contact	<input checked="" type="checkbox"/> Education Information	<input checked="" type="checkbox"/> Other

If "Other," specify or explain any PII grouping selected.

Picture, Special Access and Rank.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Describe.

The source of the PII is from the individuals' hardcopy military orders and the individual military personnel themselves, and not from any DoD, Federal or Commercial information technology systems or databases.

(3) How will the information be collected? Indicate all that apply.

- Paper Format
- Telephone Interview
- Email
- Information Sharing from System to System
- Face-to-Face Contact
- Fax
- Web Site

Other (Describe)

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Describe

Verification, Identification and Authentication of personnel with access to restricted facilities. Additionally, this application assists officials and employees of the Navy in the management, supervision and administration of Navy personnel (officer and enlisted) and the operations or related personnel affairs and functions.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe

Verification, Identification and Authentication of personnel with access to restricted facilities. Additionally, the information is used to provide Base Realignment and Closure (BRAC) data calls, alpha and social rosters, personnel recall information, Code assignments, seniority information, projected rotation/losses/gains, manning and onboard count, etc...

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

Yes

No

If "Yes," explain what risks are introduced by this data aggregation, and how these risks are mitigated?

c. Who has or will have access to PII in the DoD information system or electronic collection? Indicate all that apply.

Users

Developers

System Administrators

Contractors

Other (Describe)

Security and Military Resource Management Personnel

d. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- Security Guards
- Cipher Locks
- Identification Badges
- Combination Locks
- Key Cards
- Closed Circuit Television
- Safes
- Other (Describe)

(2) Technical Controls. Indicate all that apply.

- User Identification
- Biometrics
- Password
- Firewall
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)
- Encryption
- DoD Public Key Infrastructure Certificates
- External Certificate Authority (CA) Certificate
- Common Access Card (CAC)
- Other (Describe)

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- Methods to Ensure Only Authorized Personnel Access to PII
- Encryption of Backups Containing Sensitive Data
- Backups Secured Off-site
- Other (Describe)

e. Does this DoD information system require certification and accreditation under the DoD information Assurance Certification and Accreditation Process (DIACAP)?

Yes. Indicate the certification and accreditation status:

Authorization to Operate (ATO) Date Granted: 20061218

Interim Authorization to Operate (IATO) Date Granted:

Denial of Authorization to Operate (DATO) Date Granted:

Interim Authorization to Test (IATT) Date Granted:

No, this DoD Information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Describe.

Collection: Members PII information is collected. MILPERS data are input directly into the CDB through the web application.
Use, Retention, and Processing: Only personnel with the "need to know" can access a member's PII information.
Disclosure: No other personnel other than those with a "need to know" can access a member's PII information unless permission is granted from the individual in writing to release the information.
Destruction: Data is destroyed in accordance with the Navy's Records Management Manual.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe:

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 MILPERS, 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 MILPERS does not currently operate on the NMCI Network, but is preparing to transition to the NMCI Network, there is a risk that security controls could be disabled for maintenance and other purposes by our own maintenance personnel or NMCI personnel. The risk would be that the security controls would not be reset.

All systems are vulnerable to "insider threats." MILPERS Program Manager, System Administrators, Security Personnel and Software Programmers 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 the MILPERS Application.

These individuals have gone through extensive background and employment investigations.

Mitigation:

The following controls are used to mitigate the risks:

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 of 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. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?


Describe.

N/A

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee

Signature: 

Name: Ms. Kristin Packer

Title: Program Manager/Branch Head

Organization: SSC Pacific

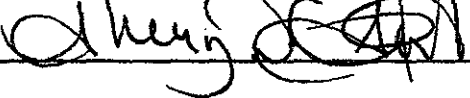
Work Telephone Number: 619 553-9641

DSN: 553-9641

Email Address: kristin.packer@navy.mil

Date of Review: 7/1/09

Other Official (to be used at Component discretion)

Signature: 

Name: CW02 Sherry Strothers

Title: MILPERS Process Owner

Organization: SSC Pacific

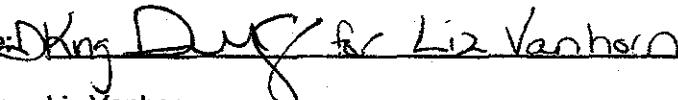
Work Telephone Number: 619-553-0295

DSN: 553-0295


Email Address: sherry.strothers@navy.mil

Date of Review: 8 Jul 09

Other Official (to be used at Component discretion)

Signature: 
Name: Liz Vanhorn
Title: Privacy Officer
Organization: SSC Pacific
Work Telephone Number: 619-553-4720
DSN: 553-4720
Email Address: liz.vanhorn@navy.mil
Date of Review: 9 July 09

Other Official (to be used at Component discretion)

Signature: 
Name: Mr. Michael McMillan
Title: Command Information Assurance Manager
Organization: SSC Pacific
Work Telephone Number: 619-553-3195
DSN: 553-3195
Email Address: michael.mcmillan1@navy.mil
Date of Review: 8 July 2009

Component Senior Information Assurance Officer or Designee

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Component Privacy Officer

Signature: miriam.brown-lam Digitally signed by miriam.brown-lam
DN: cn=miriam.brown-lam
Date: 2009.08.06 12:58:15 -0400

Name: Miriam Brown-Lam

Title: Department of the Navy Privacy Act Program Manager (DNS-36)

Organization: Office of the Chief of Naval Operations (CNO)

Work Telephone Number: (202) 685-6545

DSN: _____

Email Address: miriam.brown-lam@navy.mil

Date of Review: _____

**Component CIO Signature
(Reviewer)**



Name: Steve Muck

Title: Privacy Team Lead

Organization: Department of the Navy Chief Information Officer (DON CIO)

Work Telephone Number: (703) 614-5987

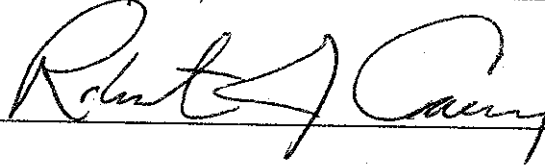
DSN: 224-5987

Email Address: steven.muck@navy.mil

Date of Review:

8/07/09

**Component CIO Signature
(Reviewing Official)**



Name: Robert J. Carey

Title: Chief Information Officer

Organization: Department of the Navy Chief Information Officer (DON CIO)

Work Telephone Number: (703) 602-1800

DSN: 332-1800

Email Address: robert.carey@navy.mil

Date of Review:

8/09/09

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection of Information. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information. Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.