



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Military Sealift Command Human Resources Management System (MSC-HRMS)

Department of the Navy - Military Sealift Command (MSC)

### **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**

N/A

**Enter Expiration Date**

N/A

**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  
5 U.S.C. Chapter 53, PAY RATES AND SYSTEMS  
5 U.S.C. Chapter 55, PAY ADMINISTRATION  
5 U.S.C. Chapter 61, HOURS OF WORK  
5 U.S.C. Chapter 63, LEAVE  
31 U.S.C. Chapter 35, Accounting and Collection  
10 U.S.C. 5013, Secretary of the Navy  
10 U.S.C. 5041, Headquarters Marine Corps  
DoD Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 8 Chapter 5  
E.O. 9397 (SSN), as amended

Additional Authorities:

5 U.S.C. Chapter 81, COMPENSATION FOR WORK INJURIES

**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.

In order for MSC to successfully carry out its mission in an ever-changing environment, MSC needs a robust resource management and staffing system to quickly and efficiently place Civilian Mariners (CIVMARS) who work and sail on the U.S. Government-owned MSC ships. MSC-HRMS resides in the Civilian HRMS sub-domain of the HRM Business Mission Area (BMA), and supports the Civilian Personnel and Pay function by providing a comprehensive and flexible tool for managing the staffing, training, and employee relations for CIVMARS. MSC's workforce goal is to attract, develop and care for a workforce capable of meeting MSC's vision. This will be achieved through an increased emphasis on career development and by promoting each individual's success by shaping, training and properly equipping the workforce. Implementing and maintaining a robust human resource management application allows the Military Sealift Fleet Support Command (MSFSC), which is charged with providing CIVMAR support and management oversight, to efficiently meet the aforementioned goals.

MSC-HRMS is a decision support mechanism to man Military Sealift Command ships and to support its mission. In order to do this, the system collects the following personal information: name, other names used, SSN, citizenship, gender, birth date, place of birth, personal cell telephone number, home telephone number, personal email address, mailing/home address, security clearance, emergency contact, Medical Information: tracks medical information for current CIVMARS and applicants. Appointment scheduling for physicals, determinations, fit for duty such including drug testing and scheduling, drug free workplace; Disability Information: tracks the fit for duty for CIVMAR (high level information); Employment Information: tracking the following information for the CIVMARS such as: terminations; disciplinary action tracking (DAT)- high level information; official personnel information; merit promotions information; separation information; CIVMAR assignments; and Education Information: tracks CIVMAR competence and position competencies such as: CIVMAR competency records, professional certification and credential data for ship assignments.

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

The Oracle Applications (Human Resources Management System) have inherent security and privacy functionality built into the product. Through the use of "Security Profiles" only those with a "Need to Know" have access to this data.

**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.

US Information Technologies (USIT) - US Citizens and have Secret Security Clearance. All Contractors are required to comply with Privacy Act and are trained annually

**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.

The PII collected is critical to ensuring the Civilian Mariner's Human Resources (HR) record is complete. Refusal to provide any/all of the mandatory PII will result in the candidate de-screening during the hiring process.

(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.

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

Civil Service Mariners are provided and sign a privacy act statement upon time of collection. The personal information collected is used for Human Resource purposes only.

**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.

Privacy Act Statement provided and signed by all new employees and at time of collection.

**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.**