

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Risk Management Informaton (RMI)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

05/14/18

SPAWAR - PMW 250

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public From Federal employees and/or Federal contractors
- From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

To collect information from active duty service members, reservist members, and members of the public on injuries and occupational illnesses required of Federal governmental agencies by the Occupational Safety and Health Administration (OSHA) and pertinent information for property damage occurring during Naval operations. The data maintained in this system will be used for analytical purposes to improve the Department of the Navy's accident prevention policies, procedures, standards and operations, as well as to ensure internal data quality assurance.

To ensure all individuals receive required safety, fire, security, force protection, and emergency management training courses necessary to perform assigned duties and comply with Federal, DoD, and Navy related regulations.

The Dive Jump Reporting System (DJRS) module of RMI collects on-duty dive and jump exposure data that allows for analysis to identify trends in personnel and equipment performance and procedural adequacy. It also serves as the source for generating official dive or jump logs for an individual or command.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

Data Matching, Verification, Identification, Administrative use

e. 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.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Yes, if the member is of the general public and involved in a Safety Incident, the member can object to the collection of PII via face-to-face meeting or via telephone.

f. 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.

Consent for use is considered given when PII is provided by the individual.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

RMI landing page presents, as required by the Privacy Act and Paperwork Reduction Act:

- 1) An OMB Control Number
- 2) A Privacy Act Advisory: "FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties."
- 3) An Agency Disclosure Notice: "The public reporting burden for this collection of information is estimated to average 1.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Information Management Division, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100 (0703-XXXX). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number."
- 4) For Face to Face and Phone Interviews: Personnel are read a "Promise of Confidentiality"

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

Within the DoD Component

Specify.

Occupational Health and Safety personnel at Ech I, Ech II, Ech III, and Ech IV Commands and activities throughout the Department.

Other DoD Components

Specify.

Force Risk Reduction (FR2), Office of the Under Secretary of Defense for Personnel and Readiness (OUSD (P&R)) Air Force.

Other Federal Agencies

Specify.

State and Local Agencies

Specify.