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

   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, DOD civilians, 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.

   See section 2, question a. for the type of information that may be collected by RMI to document injuries and occupational illnesses as described above.

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)

   Verification, identification, authentication, data matching, mission-related use, 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 is involved in a Safety Incident, the member can object to the collection of PII via face-to-face meeting or via telephone. All others cannot object since their information is pulled from other information systems.

   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 assumed when PII is provided by the individual member of the public.

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) 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."

2) 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."

3) For Face to Face and Phone Interviews: Personnel are read a "Promise of Confidentiality"

<table>
<thead>
<tr>
<th>h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Within the DoD Component</strong></td>
</tr>
<tr>
<td><strong>Other DoD Components</strong></td>
</tr>
<tr>
<td><strong>Other Federal Agencies</strong></td>
</tr>
<tr>
<td><strong>State and Local Agencies</strong></td>
</tr>
<tr>
<td><strong>Contractor</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kapsuun Group, IAW the Indefinite Delivery/Indefinite Quantity (IDIQ) Contract Number N00039-14-D-0006. Section 6.4 (Data Protection) of the Performance Work Statement (PWS) stipulates: All PMW 250 contracts contain the following language: 52.224-1 Privacy Act Notification 52.224-2 Privacy Act 52.204-21 Basic Safeguarding of Covered Contractor Information Systems &quot;The Contractor shall comply with the DON Privacy program per SECNAVINST 5211.5E. The Contractor shall ensure all categories of sensitive information, including Personally Identifiable Information (PII), are secured and in compliance with all IA Controls from the DoDI 8500.2, specifically IA Controls DCFA-1 and DCSR-2. Compliance includes the encryption of “data in transit” and “data at rest” as required by the data owner. The Contractor shall comply with DON CIO MSG DTG 171952Z APR 07 to ensure that all Personally Identifiable Information (PII) is properly safeguarded. The requirement under the E-Government Act of 2002, mandates that all PII be protected. In addition, systems processing PII must have completed a Privacy Impact Assessment (PIA) and register that PIA with DON CIO. The Contractor shall provide controlled access to prevent unauthorized access to DoD systems and information using identification and authentication as well as encryption.” Individuals have gone through an extensive background and employment investigations and only those personnel with &quot;Need to Know&quot;.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Individuals</strong></td>
</tr>
<tr>
<td><strong>Existing DoD Information Systems</strong></td>
</tr>
<tr>
<td><strong>Databases</strong></td>
</tr>
<tr>
<td><strong>Commercial Systems</strong></td>
</tr>
</tbody>
</table>

DD FORM 2930, JUN 2017
Other Federal Information Systems:

Existing DoD Information Systems:

Joint Deficiency Reporting System (JDRS)
Enterprise Safety Application Management System (ESAMS)
Marine Sierra Hotel Aviation Readiness Program (M-SHARP)
Defense Civilian Personnel Data System (DCPDS)
Defense Manpower Data Center Reporting System (DMDCRS)
Marine Corps Medical Readiness Reporting System (MRRS)
Aeromedical Services Information Management System (ASIMS)
Medical Protection System (MEDPROS)
Corporate Enterprise Training Activity Resource Systems (CeTARS)
Naval Aviation Logistics Command Management Information System (NALCOMIS)
Decision Knowledge Programming for Logistics Analysis and Technical Evaluation (DECKPLATE)
Defense Civilian Payroll System (DCPS)
Global Combat Support Systems- Marine Corps (GCSS-MC)
Injury Verification Feed (IVF)
Marine Corps Total Force System (MCTFS)
Total Force Structure Management System (TFSMS)
Enterprise Safety Application Management System (ESAMS)
Enterprise Safety Applications Management System (ESAMS) - Injury/Illness Reporting and Tracking System (IIRTS)
Force Risk Reduction (FR2)
Joint Deficiency Reporting System (JDRS)
Person-Event Data Environment (PDE)
Medical Mishap and Compensation Systems (MMAC)
PNS Occupational Accident and Injury Reporting System (POAIRS)
Defense Injury and Unemployment Compensation System (DIUCS)
Enterprise Resource Planning (ERP)
Graduate Training Integration Management System (GTIMS)
Marine Corps Training Information Management System (MCTIMS)
Defense Finance and Accounting Service (DFAS)
Division of Longshore and Harbor Workers' Compensation (DLHWC)

j. How will the information be collected?  (Check all that apply and list all Official Form Numbers if applicable)

- E-mail
- Face-to-Face Contact
- Fax
- Information Sharing - System to System
- Other (If Other, enter the information in the box below)

Members of the public: face-to-face and telephone interview
Government (military, federal, contractor, reservist): pulled from other information systems

k. 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 must be consistent.

- Yes
- No

If "Yes," enter SORN System Identifier: DMDC 02 DoD; NM05100-4; NM05100-

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpclid.defense.gov/Privacy/SORNS/
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

Note: SORNS - DMDC 02 DoD; NM05100-4; NM05100-5; F032 AF ILE; NM06150-6
A "Risk Management Information" SORN is in development and once published will act as the sole authority for the system.
I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

|GRS 1.34|

(2) If pending, provide the date the SF-115 was submitted to NARA.

|m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.

(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN DMDC 02 DoD, Defense Enrollment Eligibility Reporting Systems (DEERS) (July 27, 2016, 81 FR 49210), authorities:

SORN NM05100-4, WESS Occupational Injuries/Illnesses System (November 16, 2004, 69 FR 67128), authorities:
10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; E.O. 9397 (SSN); E.O. 12196, Occupational Safety and Health Programs for Federal Employees; DoD Instruction 6055.7, Accident Investigation, Reporting, and Record Keeping; OPNAVINST 5102.1 series, Mishap Investigation and Reporting; and MCO P5102.1B, Marine Corps Ground Mishap Investigation and Reporting Manual.

SORN NM05100-5, Enterprise Safety Applications Management System (ESAMS) (March 25, 2011, 76 FR 16739), authorities:

SORN F032 AF ILE, Enterprise Environmental, Safety and Occupational Health-Management Information System (EESOH-MIS) (December 19, 2005, 70 FR 75157), authorities:
10 U.S.C. 9832, Property Accountability: Regulations; and E.O. 9397(SSN).

SORN NM06150-6, Medical Readiness Reporting System (MRRS) (August 23, 2013, 78 FR 52518), authorities:
10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; BUMED Note 6110, Tracking and Reporting
n. Does this DoD information system or electronic collection have an active and approved 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  - [ ] No  - [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

<table>
<thead>
<tr>
<th>OMB Control #</th>
<th>Risk Management Information (RMI) System</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>0703-0065</td>
<td>Risk Management Information (RMI) System</td>
<td>09/30/2022</td>
</tr>
</tbody>
</table>