PRIVACY IMPACT ASSESSMENT (PIA)

For the

Risk Management Information (RMI)
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** ☐ **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: 16398 ; DITPR DON ID 22841

☐ **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 007-000006663

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 DMDC 02 DOD; DMDC 12 DOD;NM1640-1; NM03750-1

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	PENDING: PROCESS INITIATED BY COMPONENT
Enter Expiration Date	PENDING

☐ **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.

5 U.S.C. 41 4101-4118, "The Government Employees Training Act of 1958"

5 U.S.C. §301, "Departmental Regulations"

10 U.S.C. §5013, "Secretary of the Navy"

10 U.S.C. §5041, "Headquarters, Marine Corps"

E.O. 12196, "Occupational Safety and Health Programs for Federal Employees"

DoD Instruction 6055.07, "Mishap Notification, Investigation, Reporting, and Record Keeping"

OPNAVINST 5102.1D/MCO P5102.1B, "Navy & Marine Corps Mishap and Safety Investigation, Reporting, and Record Keeping Manual"

OPNAVINST 3750.6S, "Naval Aviation Safety Management System"

DoD 6025.18-R, "DoD Health Information Privacy Regulation"

E.O. 9397 (SSN), as amended.

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.

To collect information 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.

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

To protect privacy, and mitigate the risks associated with the collection and storage of PII, the following safeguards are implemented:

1) The RMI web application is public key enabled (PKE), requiring a valid and current DoD PKI certificate for access

2) Servers are located within limited access areas of a controlled, DoD facility, and all personnel with physical access to the servers have the training required for handling Privacy Act data and systems of records. Remote access is limited to users with a bonafide need-to-know that have obtained the required security clearance and Cybersecurity Workforce training and certification.

3) Paper records are being safeguarded in locked enclosures within protected spaces

4) All data-at-rest is encrypted on the database

5) All data-at-rest that is stored on a thin client is encrypted

6) All data transmissions are encrypted, both to and from the database

7) Workflows built into the program prevent unauthorized users from viewing others' PII

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. Commands and activities throughout the Department of the Navy required to report safety mishaps and injuries.

Via bi-directional interface/data exchange:
-All Weapons Information System (AWIS), NAVSEA

☒ **Other DoD Components.**

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

☒ **Other Federal Agencies.**

Specify. Occupational Safety and Health Administration (OSHA)

☐ **State and Local Agencies.**

Specify.

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

Specify. Syneren Technologies Corporation, 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:

"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."

☐ **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 directly 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 directly from the individual.

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.

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."

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.