PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Safety Applications Management System (ESAMS)
Department of the Navy - CNIC

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: DITPR ID: 4763 DITPR DON ID: 20927
- ☐ **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 UII: 007-000001526

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 NM05100-5

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

Enter Expiration Date

☐ **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 NM05100-5 authorities:

5 U.S.C. 4101- 4118, the Government Employees Training Act of 1958;
10 U.S.C. 5013, Secretary of the Navy;
10 U.S.C. 5042, Commandant of the Marine Corps;
E.O. 12196, Occupational Safety and Health Programs for Federal Employees;
DoD Instruction 6055.7, Accident Investigation, Reporting, and Record Keeping;

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 provide a mechanism for personnel, supervisors, department coordinators/administrators, command administers, regional administrators, claimant administrators, and commands providing base operational support (BOS) administrators, a system to track information that supports compliance for but is not limited to:
- Workplace or building inspections (occupational safety, traffic safety, recreational off-duty safety, explosive safety, radiation safety, fire safety, environmental, etc.)
- External agency inspections related to occupational safety, emergency management, fire, security, etc.
- Deficiency tracking (such as workplace, building, process, etc.)
- Corrective action tracking
- Occupational injuries or illnesses and off-duty injuries for military personnel only
- Property Damage related mishaps
- Near Miss Incidents
- SF-91 reporting and tracking
- Lessons Learned
- Training - computer-based-training, classroom, on-the-job, and formal
- Equipment tracking and associated inspections, maintenance, and testing associated with each item
- Equipment tracking allocations
- F&ES Vehicle tracking
- Area hazard tracking (such as confined spaces, noise hazard level, sight hazards, etc.) and associated inspections, maintenance, and testing associated with each item.
- Fire incident reporting
- Command or department level self-assessments
- Unsafe/unhealthful reporting and administration
- Hot works permit tracking
- Fire facility related data and fire pre-plan information
- Drill schedules
- Training schedules
- Job hazard analysis
- Respirator fit-testing and management
- Personnel surveys
- Occupational medical surveillance information
- Assigned duties/tasks with associated training
- Personnel listings
- External enrollment in training
- Duty Rosters for fire personnel
- Daily activity log for Fire and Emergency Services (F&ES)
- Anti-Terrorism and Force Protection (ATFP)
- Firing Range Management and Scheduler
- Small arms weapons qualification training and tracking

To ensure all individuals receive required training, medical surveillance, respirator fit-tests, certifications in the ares of occupational safety, public safety, traffic safety, recreational and off-duty safety (military personnel only) fire and emergency services, security, emergency management, Naval Air Training and Operating Procedures Standardization (NATOPS), environmental, and other mandated training, necessary to perform assigned duties and comply with Federal, DoD, and Navy related regulations.

In addition, to track all DoD sponsored traffic training and related required training for the use of motorcycles on or off-base by military personnel and civilian personnel on base only.

Personal information collected: Name, Other ID: DoD ID Number, Gender, Birth Date, Mailing/Home Address, Marital Status, Employment Information: grade/rank, series/specialty, service/status, hire date,

Note: Home address is not collected on all individuals. Only those individuals who have a mishap and an

associated OSHA 301 form completed.

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

PII is collected and stored in ESAMS, a securely hosted web based system. PII data is displayed on workstation monitors. All HGW employees that use ESAMS must take information assurance training. To avoid compromise, workstation machines "time out" and monitors darken if periods of inactivity are exceeded. This keeps unattended workstations from being left for long periods with data exposed.

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. Occupational related injuries and illnesses and off-duty military injuries are shared with the Naval Safety Center's Web Enabled Safety System (WESS); Training data is shared with Navy Training Management and Personnel System (NTMPS); Military personnel data is received from Navy Standard Integrated Personnel System (NSIPS). Data is only received from DEERS.

☒ **Other DoD Components.**

Specify. Proposed - Mishap data for DoD components will be fed to the DoD system Force Risk Reduction.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. HGW and Associates, LLC contractor, required to protect privacy according to the privacy act of 1974. The contract with HGW contains the required FAR Privacy Clauses

☐ **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 individual can object, however, failure to provide the requested information may result in inability to participate in required safety and emergency training courses.

(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.

Once the individual provides their information they are consenting to its use for training purposes.

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 Advisory and a Privacy Act Statement are provided to users online prior to login on the ESAMS web site and 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 may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.