PRIVACY IMPACT ASSESSMENT (PIA)

For the

Data Housing And Reports Tool (DHART)
Department of the Navy - United States Marine Corps (USMC)

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	13957
☐	**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 NM01500-2

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

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.

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps: function, composition; OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS), Catalog of Navy Training Courses and Student Reporting Requirements; MCO 1580.7D Schools Inter-service Training; and 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.

DHART is a thin client training data application that provides tracking of student records for Commandant of the Marine Corps, Plans, Policy & Operations (PP&O), Security Division, Law Enforcement Branch (PSL), 2111 Eisenhower Avenue, Alexandria, VA 22314. POC name: Mr. Jeff Johnson, YN3, Head, Supporting Establishment Law Enforcement. The purpose of this system is to record course and training demands, requirements, and achievements; analyze student groups or courses; provide academic and performance evaluation in response to official inquiries; provide guidance and counseling to students; prepare required reports; and for other training administration and planning purposes.

The personal records include: Name, truncated Social Security Number, gender, personal cell phone number, rank/rate/grade, branch of service, billet, military occupational specialty (MOS), Work Section within their Military Police Departments, Assigned Military Police Departments, subspecialty codes, and educational information.

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

Privacy data is handled in accordance with the Privacy Act and the system complies with FISMA/DIACAP requirements. Role-based access controls are used for controlling access to the system using the policy of least privilege, which states that the system will enforce the most restrictive set of rights/privileges or access need by users based on their roles. They create roles for each level of access required for employees to perform their job functions and follow procedures including security and privacy training, and need-based job responsibility. DHART limits dissemination of USMC PII only to those with a business need to know, to minimize the risk of data misuse.

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. Contractor : Homeland Security Solutions, Inc (HSSI). All contractors are bound by the Privacy Act. From the Contract: "HSSI is in full compliance with SECNAVINST 5211.5E in the collection and storage of Personally Identifiable Information (PII) to include documentation, training, and IT processes. The contractors have taken the

necessary steps to be included in the DOD System of Records, listed within NM01500-2 (DON) Training and System Record."

☐ **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.

When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement (PAS) is required regardless of the medium used to collect the information (paper or electronic forms, personal interviews, telephonic interviews, or other methods). The statement enables the individual to make an informed decision whether to provide the information requested. Personal information obtained without a PAS shall not be incorporated into any system of records.

The following disclosure is within this form: "Provision of the requested information is voluntary. However, failure to provide the information may result in your training not being properly recorded in your training file which may impact your qualification as a military policeman/police officer and for staffing to certain billets."

(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.

Individuals are informed of the purpose for collection of their PII within the Privacy Act Statement and give their consent upon the signing of such form.

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

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.

Each and every time an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement (PAS) is required. The statement enables the individual to make an informed decision whether to provide the information requested. Personal information obtained without a PAS shall not be incorporated into any system of records.

The following information is offered to each individual within the Marine Corps Police Student Information form:

AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps.

PRINCIPAL PURPOSE: Information collected by this form will be used by the Commandant of the Marine Corps (PSL) and installation Provost Marshal's Offices/Marine Corps Police Departments to document required Marine Corps training.

RETENTION: The collected information will be maintained in an electronic database and in hard copy training records for the Commandant of the Marine Corps (PSL) and installation Provost Marshal's Offices/Marine Corps Police Departments with restricted, limited access permissions and password protections in place. Records in this file system will be retrieved by record subject name and will be destroyed after an individual leaves the Marine Corps or employment with the Marine Corps, or when no longer needed, whichever is later. DHART records are retained for the duration of employment/service plus 30 years and then destroyed.

ROUTINE USES: None other than the blanket routine uses established by the Department of Defense Privacy Office and posted at http://www.defenselink.mil/privacy/notices/blanket-uses.html. Maintenance of this information is authorized and governed by Privacy Act System of Records Notice NM01500-2 Department of the Navy (DON) Education and Training Records (November 22, 2005, 70 FR 70594) posted at http://www.privacy.navy.mil/privacy/noticenumber/NM01500-2.doc.

DISCLOSURE: Provision of the requested information is voluntary. However, failure to provide the information may result in your training not being properly recorded in your training file which may impact your qualification as a military policeman/police officer and for staffing to certain billets.

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.