PRIVACY IMPACT ASSESSMENT (PIA)

For the

Civilian Workforce Development Application (CWDA)
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	
☐	**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 M12400-1 Civilian Workforce Development Application

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.

(1) 10 U.S.C. 5013, Secretary of the Navy
(2) 10 U.S.C. 5041, Headquarters, Marine Corps
(3) 5 U.S.C., Section 301, Departmental Regulations
(4) MCO 12510.2C, Civilian Workforce Management
(5) MCO 12713.6A, Equal Employment Opportunity Program
(6) MCO 12451.2C, Honorary Awards for Civilian Employees
(7) MCO 12301.1B, Authority to Approve Extensions to the DoD 5-Year Overseas Employment Limitation and Movements Between Overseas Areas for Civilian Employees
(8) MCO 12410.21B, Consolidated Civilian Career Training (CCCT) Program
(9) 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.

CWDA is a web-based COTS tool, the primary purpose is to facilitate the occupational and professional development of Civilian Marines. The database contains Civilian Marine personnel data and data related to the leadership and core competencies of the Communities of Interest (COI's). CWDA provides career and professional development information to Civilian Marines and allows them to schedule training, update personal training/qualification data, and view job vacancies within the Marine Corps.

The type of information CWDA collects includes information about the COI's, the occupational series allocated to each COI, and professional development information for each occupational series, to include functional and leadership competencies necessary for the performance of occupational series-related duties, professional development attributes related to career development, and training opportunities available to occupants of occupational series.

The PII included in CWDA: Name, Social Security Number (SSN), citizenship, gender, race/ethnicity, birth date, place of birth, home phone number, e-mail address, mailing address, security clearance, marital status, salary information, disability information and education information.

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

CWDA, as well as many information technology systems, has potential privacy risks. CWDA addresses safeguards to privacy by controlling functionality and data by defined user roles. CWDA is used by Civilians and authorized DoD personnel, and any PII that is shared or released is done so with the express written permission of the individual concerned using the standard Privacy Act Statement Release Form. CWDA is vulnerable to privacy threats such as environmental effects, information warfare, sabotage, or localized disruptions caused by physical attacks and destruction as well as records loss or unauthorized update/modification of records in the system.

CWDA will enforce the requirements to protect sensitive data. This will include controlling access to CWDA applications and software by using identification and authentication mechanisms (e.g., user ID's and passwords or Common Access Card (CAC) and secured by public key infrastructure (PKI)), discretionary access control, object reuse, and auditing. Depending on the level of access required, official users may have one or more roles. Unauthorized access or intrusion into the CWDA network may occur; however, this intrusion is unlikely due to the inherent security procedures. Once every three months a security audit is done on all CWDA servers. Access to data in CWDA is only provided to official users with legitimate billet requirements and receives mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII resident in CWDA.

In addition, contractors receive an annual security briefing and compliance quiz which includes safe handling of PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data. Physical access to the servers is controlled by M&RA, Manpower Information Technology (MIT).

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. System: Department of Navy Civilian Authority Data Source (DONCADS)
System Owner_Jointly: United States Navy (USN) Office of the Chief of Naval Operations (OpNav), Manpower & Reserve Affairs (M&RA)

System: Non-Appropriated Fund Instrumentality System PeopleSoft Human Resources Information System (NAFI)

System Owner_Jointly: Marine Corps Community Services (MCCS) and Marine Corps Systems Command (MCSC)

☒ **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. Contractors are bound by the rules and laws of the Privacy Act. Contractors sign a Non Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information. Specific language in the contract is described as:

Security measures shall be taken to satisfy the security requirements in accordance with the Marine Corps System Security Plan. CWDA data/information shall be protected from an Information Systems Security (INFOSEC) perspective. The contractor shall apply security considerations to software design and management.

Only contractors who have a valid need to know and a favorably adjudicated background investigation are permitted to have access to CWDA. During the course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting the DoD.

☐ **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 directly entered or collected into CWDA by official users. CWDA is used exclusively by Civilian and authorized DoD personnel. If an individual objects to the collection of PII then they may contact the NAFI and DONCADS systems owners to have their data removed from those systems.

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.

As data is shared from the centralized manpower databases individuals are not provided the opportunity to consent to specific uses of their PII. Although Civilian Marine's do not have the opportunity to consent or object to PII within CWDA, they do have the opportunity to its use in DONCADS or NAFI at anytime.

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.

All CWDA official users receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard PII. In addition, contractors who have access to the system, also receive an annual security briefing conducted by their companies Facility Security Officer (FSO) which includes safe handling of PII. These annual PII sessions include safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

All CWDA official users are required to read and acknowledge a Privacy Act Warning (PAW) which notifies the official user that they are entering into a system that is governed by rule-making established by the Privacy Act of 1974 [5 U.S.C. 552a] and that mandated safeguarding, handling and disposal procedures must be observed. The PAW further apprises the official user that they are not allowed to share or disseminate PII from CWDA unless authorized by law and that civil and /or criminal penalties will apply. However, CWDA currently does not have the pop-up PAW functionality implemented. The CWDA Project Officer and Functional Manager will work with the vendor to develop and implement the PAW pop-up functionality. A risk and mitigation strategy will be included in the CWDA Plan of Action & Milestones (POA&M).

Currently CWDA does not collect PII directly from an individual or (Records Subject). CWDA only receives PII from the DoNCADS and NAFI systems listed in Section 3, para (2) of this PIA. Should a future requirement to collect PII from a Records Subject arise, the CWDA Functional Manager in

coordination with the Marine Corps Systems Command (MCSC) CWDA Project Officer will evaluate the requirement and its associated PII risks within CWDA and ensure any known risks are mitigated through the CWDA Change Control Board (CCB). Should the requirement be approved for implementation within CWDA, this PIA and its associated SORN will be evaluated and updated, as needed, to reflect the change in PII collection. Lastly, the Privacy Act Statement (PAS) notification procedures and inclusion of a PAS "pop-up" screen in CWDA is mandated to be implemented at the same time the functionality to collect PII from a Records Subject is implemented within CWDA.

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.