PRIVACY IMPACT ASSESSMENT (PIA)

For the

Total Information Gateway Enterprise Resources

Marine Corps System Command

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 1237

☐ **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 007-17-01-16-02-1665-00

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 M06320-1 Marine Corps Total Information Management Record

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.

10U.S.C. 5013
Secretary of the Navy; 10U.S.C. 5041
United States Marine Corps; 5 U.S.C. 301
Departmental Regulations: E.O. 10450
Security Requirements for Government Employment; and E.O. 9397 (SSN)

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.

Purpose: The Total Information Gateway Enterprise Resources (TIGER) is an over-arching umbrella of individual business process improvement systems used internally at Marine Corps Systems Command (MCSC).

The system within TIGER which uses Personally Identifiable Information (PII) data is the Staff Directory module. Staff Directory is the Command's Human Resources database which tracks civilian and military employee information and makes the necessary information available to various organizations within MCSC. Each sub-section of the Staff Directory automates an otherwise paper based business process. These sub-section range from parking stickers to billet management, from Recall Roster generation to Individual Development career tracking.

Information is entered into the application through a web based interface during the user's inbound process as they are assigned to MCSC as an employee. During the check-in process the following information is inputted or updated by the individual.

SSN - View only (for verification)
First Name - Employee is be able to edit this field if necessary
Middle Name - Employee is be able to edit this field if necessary
Last Name - is be able to edit this field if necessary
Rank
Date of Rank - Date the employee achieved current Grade/Rank
Race
Gender
Date of Birth – Date of Birth is required for incoming employees. The employee must be at least 15 years old
Place of Birth
Spouse
AFADBD (Armed Forces Active Duty Base Date, The date the marine joined the military)
Personal Address Information
Address
Phone

Home address and spousal information are collected to provide information to the Recall Roster which provides a Point of Contact (POC) in case of emergency.

In addition to other personal information Gender and Race are used as part of NSPS training reporting as required of the Command.

Personal information such as Social Security Numbers (SSN) are stored as a reference for the Workforce Management and Development (WMD) individuals who have to manually enter that information into external systems such as 3270, DCPDS and ODSE.

3270 is a software application which allows user to connect to other mainframes from their desktop client. MCSC use this application to process in-bound/out-pound reports for accountability.

DCPDS – DCPDS (Defense Civilian Personnel Data System) is a human resources information system that supports civilian personnel operations in the Department of Defense (DoD). It covers all DoD civilian employees: appropriated fund, non-appropriated fund, and local national employees.

Operational Data Store Enterprise (ODSE) is an Oracle database that represents the current snapshot of all the data in the Marine Corps Total Force System (MCTFS).

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

Privacy of PII is of critical importance to the employees and the Command. Managing the risk to prevent the release of PII is the responsibility of the application owners and the individual employees who access and utilize that information. The risks are mitigated by the application of a strict access security model and training. The following briefly describes steps taken in more detail:

Access to the information is controlled through a strictly enforced, roles based security model. The number of necessary users with access to the PII is kept to a minimum by close monitoring of the role allocation. Administrative access to the application is required to modify the roles based security model.

Physical security to the MCSC owned and managed servers is only allowed through a permanently locked door and requires prior authorization from the Command Data Center Manager. Server administrators possess a Top Secret clearance as per Command/DoD policy.

Access to TIGER/Staff Directory is provided on a need to know basis and via a valid CAC and Public Key Infrastructure (PKI) enabled authentication. All TIGER users (to include contractors) receive mandatory Marine Corps sponsored Privacy Act and PII protection and spillage training annually to help safeguard the PII resident in TIGER.

MCSC provides mandatory internal security training for all employees and all contractor companies are required to provide a similar brief to its employees. This training includes safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding of PII data.

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. None

□ **Other DoD Components.**

Specify. None

□ **Other Federal Agencies.**

Specify. None

□ **State and Local Agencies.**

Specify. None

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

Specify. None

□ **Other** (e.g., commercial providers, colleges).

Specify. None

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.

During the check in process, individuals have the ability to question the requirements for the collection of the PII but the fields are mandatory and must be filled out to complete the check-in process.

PII is required for training and workforce management. While PII must be collected, individuals are able to correct erroneous information resident within TIGER. PII for Marines is pulled from ODSE and for government civilians pulled from DCPDS. The PII for others are manually entered by administrators when the are registering for training.

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 information is only used for specific DoD mandated requirements.

PII resident in TIGER is used to provide training management and workforce management for the individuals within MCSC. If a Marine or government civilian were given the opportunity to exclude their PII from TIGER, it would prevent the accurate record keeping of training Marines have completed, causing possible delay in advancement. Required training such as PII, Security, Ethics, and NSPS are reported entered into to ODSE and DCPDS as a matter. of record.

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: PRIVACY ADVISORY:

applicable format.	The TIGER Program Manager is working with to create a TIGER Privacy Advisory Warning for all TIGER users to acknowledge each and every time a user logs into TIGER. This PIA will be amended once the PAS is published.

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.