PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Fish & Wildlife Conservation Tracking System (EFAWCTS)
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 NM05580-1

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

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
E.O. 9397 (SSN)
MARADMIN 533/08, "Internal Housekeeping"
SECNAV M5210.1, SSIC 5580 Law Enforcement Records

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.

The purpose of eFAWCTS is to support the fish and wildlife user, as well as the Conservation Law Enforcement Office (CLEO) staff. It will be a robust, portal-based system that allows the user to access a site and apply for Base permits, take required tests, view availability of recreational areas,request to open or close a hunting or wood cutting session, view instructional and educational material, and report harvest information. The user will be required to login to apply for permits, request to open or close a session, report harvest information, take tests, or view availability of hunting areas.

Types of personal information that a user enters in the system include: Name; Home Address; Personal Email; Contact Phone Numbers; Date of Birth; State Driver's License information; Hunting, Fishing, Trapping license information; and Vehicle information.

CLEO staff users enter Case Violation data that includes: Social Security Number, Date of Birth, Name, Address, Phone, Gender, Height, Weight, Eye Color, Hair Color, and Race. Case Violation data is only accessible to CLEO staff users.

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

The information collected is deemed "unclassified data," such as names, Social Security numbers and home addresses, this data is however, vulnerable to possible database break-in/hacking and insider threats (i.e., malware, worms, and disgruntled employees seeking revenge or inadvertent human error).

General protection measures, privacy-specific protection measures, and security controls are used to help safeguard privacy, such as: creating policies and procedures for protecting the confidentiality of PII; conducting training by requiring that all users receive appropriate training before being granted access to organization information systems; using access enforcement to control access to PII through access control policies and access enforcement mechanisms (i.e., access control lists); providing transmission confidentiality to protect the confidentiality of transmitted PII, which is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted; and auditing events to monitor events that affect the confidentiality of PII, such as inappropriate access to 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. U.S. Marine Corps

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☒ **State and Local Agencies.**

Specify. Violation data is shared with state and local authorities during court proceedings.

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

Specify.

☐ **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.

User is asked to agree to terms and conditions of the site before logging in.

(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.

The subject individual initiates the collection and maintenance of his/her information for the purposes of:

applying for base hunting permit/license,
obtaining access to view availability of areas for recreational use, and
check-in and check-out of hunting/recreational areas. Release of this information is done with the individual's full cooperation and consent.

(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.

There is a Privacy Act Warning (PAW) Pop-up screen for all users to acknowledge, each and every time a user logs in.

Privacy Policy

1. This is an official United States Marine Corps website, and is provided as a public service by the *Marine Corps Base Public Affairs Office.*

2. Information presented on this site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with (National Archives and Records Administration General Schedule 20). All data collection activities are in strict accordance with DoD Directive 5240.1 (reference (p)).

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

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.