PRIVACY IMPACT ASSESSMENT (PIA)

For the

RecTrac, et. al
FAMILY & MORALE WELFARE AND RECREATION 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	3815 (DA05843)
☐	**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 A0215 FMWRC

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.

Statutory: 10 U.S.C. 3013, Secretary of the Army; 26 U.S.C. 6041, Information at Source; Army Regulation 215-1, Morale, Welfare and Recreations Activities and Non-appropriated Fund Instrumentalities; Army Regulation 215-3, Non-appropriated Fund Personnel Policy; Army Regulation 215-4, Non-appropriated Fund Contracting; Army Regulation, 608-10 Child Development Services; DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR); DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR); 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.

The purpose of the RecTrac application is to register households/family members for access to Army recreation and child development programs/services IAW DA regulatory requirements (to include tracking program usage, processing payments, monitoring eligibility/child health requirements and facilitating annual demographics/management reporting) and to maintain records for staff, volunteers, instructors and Family Day Care providers (to include background data, training records, operational requirements, certifications, etc). The types of personal information collected consists of sponsor/staff/instructor/provider personal information; class rosters; activity schedules; pass management files; facility usage data; staff/provider/ instructor information, qualifications, training and background checks; resale goods inventory, product pricing, menus; rental equipment records, hold harmless agreements for rental contracts; reservation information; account balance information and revenue from sales data.

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

The potential for identity theft and unauthorized use of the data by unauthorized personnel exists even with the security provided. The data is encrypted, access to information is controlled by User-ID and password, user transaction logs maintained and Novell security system is in place. Data is not released to any parties other than sponsor (Uniformed/Participating Head of Household). However, the security measures in place within the security configuration of the system and on the NIPRNET, are in accordance with best practice and due diligence.

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. Primarily within Army Garrisons, but initiatives to include National Guard are being worked for ease in transition of a Soldier/Family from Guard to Active Duty then back to Guard.

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. National Agency Background Check for staff/providers/some instructors

☒ **State and Local Agencies.**

Specify. State-based Dept of Agriculture and child care assistance programs for purposes of financial aid or reimbursement for eligible families or programs. Program partnerships with local youth organizations (Boys & Girls Clubs of America, 4-H Club).

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

Specify. Agreement on file (G6) with Contractor that data will be safeguarded, data will not be loaded or transported on mobile devices, data will be deleted and purged off the ftp site, and all employees are briefed on the safeguarding of PII information.

☐ **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.

During the initial data collection interview, the individual is provided with the Privacy Act Statement and informed that providing the information is optional and that failure to provide the information may result in slow or denied services. The purpose of collecting data and its uses are described and the individual has the right to refuse to provide the information.

(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.

A Privacy Act Statement is provided at the time the data is collected.

(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.

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.