PRIVACY IMPACT ASSESSMENT (PIA)

For the

Case Management and Tracking System
Defense Human Resources Activity

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	8243
☐	**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 007-97-01-03-02-3866-00

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 OPM/GOVT3

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.

5 U.S.C. 3321, 4303, 7504, 7514, and 7543

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.

These records result from the proposal, processing, and documentation of these actions taken either by the Office or by agencies against employees in accordance with 5 CFR parts 315 (subparts H and I), 432, 752, or 754 of the Office's regulations.

The CMTS is intended to provide case tracking and management for employee and labor relations cases. Electronic case files and reports capability for trend analysis and to target training needs and other program improvement efforts. The only Privacy Act data collected on individuals is the name, DOB, employment information and SSN of the employee to whom the case applies, and the names of the various management and union representatives. The only information collected about non-Federal employees will be the names and business addresses of national level union officials and private attorneys. This information is currently collected in paper and spreadsheet form. CMTS allows for the electronic collection of this same data.

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

The risk to an individual is that his/her name, DOB, employment information and SSN could be associated with a particular case. This is the same risk that currently applies to these case files in their paper state. The CMTS information is encrypted, only accessible to authorized users with a bona fide need-to-know. User authorizations are role based, require a two-step approval process, and provide access through common access card log-in, with back up user name/password log-in which conforms to DoD password credentials.

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. Authorized individuals in all DoD Agencies

☒ **Other DoD Components.**

Specify. Army, Navy, Air Force, Defense Agencies, i.e., DLA, DCMA, DFAS, WHS, et al.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

The use of the individual name(s), SSNs, employment information and DOB are required for the records pertaining to him/her, in order to allow for proper case adjudication, including to make appropriate contact with individuals necessary to obtain testimony, process case actions, inform individuals of requirements, meetings, etc.

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 stated above the names, SSNs, employment information and DOB of individuals are required for identification of cases to ensure appropriate adjudication and processing. Management has a statutory right to assign work to individuals and to evaluate that work; CMTS is a tool by which management makes and monitors assignments to LER practitioners. In addition, employees who are a party to a case have no authority to dictate nor right to consent to management's taking appropriate employment actions and documenting those actions in accordance with governing law, rule, and regulation. This disclosure is part of routine Federal Human Resources data collection.

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.	Individuals are not asked to provide their own privacy information as part of case processing. The only private individual information used in CMTS is the name, SSN, employment information and DOB of individuals as part of LER case processing which will be obtained via extract file from DCPDS, or by content of an SF-50. This privacy information will be obtained as either the object of a discipline, adverse or performance-based action, appellant, or in their official capacity as a witness, case practitioner, attorney, manager, supervisor, etc. All CMTS users will receive notice that the system contains personal identifiable information which must be protected according to law, rule and regulation. CMTS access to the data is limited by role designation to those with an appropriate need to know.

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.