PRIVACY IMPACT ASSESSMENT (PIA)

For the

<table>
<thead>
<tr>
<th>FTDTL-IMS - FORENSIC TOXICOLOGY DRUG TESTING LABORATORY-INFORMATION MANAGEMENT SYSTEM (IMS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Army Medical Command (MEDCOM)</td>
</tr>
</tbody>
</table>

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

UII: 007-000009991

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

DMDC 01

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.

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 Forensic Toxicology Drug Testing Laboratory - Information Management System (FTDTL-IMS) is the DoD umbrella system of applications required to implement the Congressionally-mandated testing of military and select government civilians for the presence of illegal drugs. It supports the DoD drug deterrence program for the readiness of the military forces and operates in facilities/units of the Drug Deterrence Office (DDO). FTDTL-IMS provides a database to automate the tracking and documenting of urine specimens through the drug testing and validation process from the time the urine specimen is taken until final disposition of the specimen. This system records the identification of all laboratory personnel and tests being performed at each stage of the testing and validation process. Specimens and positive test data remain at each drug-testing laboratory pending resolution of positive test results. The positive test results may be used in litigation and the collection of PII is required to maintain accurate records of the test results.

This PIA covers the following FTDTL-IMS components:
- Forensic Toxicology Drug Testing Laboratory – Web Reporting System (FTDTL-WRS)
- Drug Testing Program - Client Collection System (DTP-CCS)
- Laboratory Information Management System (LIMS)

The categories of individuals covered by this system include: Active duty Army, Navy, Air Force, Marine Corps, and Coast Guard officer and enlisted personnel; members of a reserve component; individuals examined to determine eligibility for military service at an Armed Forces Entrance and Examining Station; DoD civilian employees; Reserve Officer Training Corps (ROTC) and Service academy cadets who are tested as part to their entrance into these programs and schools; and foreign nationals who are employed by DoD or attending US military training schools.

The categories of records in this system include: Military drug test records containing the Social Security Number (SSN) or DoD ID number, date of specimen collection, date test results reported, reason for test, test results, base/area code, unit, service, status (active/reserve), and location code of testing laboratory.

This PIA updates the previous PIA approved on 8 April 2014.

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

The privacy risks associated with the PII collected include unauthorized access to PII, inaccurate PII in the system, and unauthorized disclosure of PII. There are administrative, technical, and physical security measures in place to mitigate these risks as indicated in Section 3 below.

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.

- [x] Within the DoD Component.
  Specify. PII is shared with authorized personnel in Army organizations.

- [x] Other DoD Components.
Specify. PII is shared with authorized personnel in the Navy, Marine Corps, and Air Force organizations as well as the Military Entrance Processing Command (MEPCOM), Reserve Officer Training Corps (ROTC), Cadet Commands, and Service academies.

☑ Other Federal Agencies.

Specify. PII is shared with authorized personnel in the Coast Guard organizations.

☐ State and Local Agencies.

Specify.

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

Specify. AllientCorps. There are clauses in the contract requiring adherence to the Privacy Act, Title 5 of the US Code, Section 552a and other applicable agency rules and regulations that require the protection and confidentiality of personal 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.

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

The individual does not participate in the collection of PII for this system. PII is collected from existing DoD information systems, applications, and databases (unit rosters).

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.

The individual does not participate in the collection of the PII for this system. PII is collected from existing DoD information systems, applications, and databases (unit rosters).

<table>
<thead>
<tr>
<th>k. What information is provided to an individual when asked to provide PII data?</th>
<th>Indicate all that apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Privacy Act Statement</td>
<td>[ ] Privacy Advisory</td>
</tr>
<tr>
<td>[ ] Other</td>
<td>☒ None</td>
</tr>
</tbody>
</table>

Describe each applicable format.

The individual does not participate in the collection of the PII for this system. PII is collected from existing DoD information systems, applications, and databases (unit rosters).
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.