PRIVACY IMPACT ASSESSMENT (PIA)

For the

TACOM LCMC Account Control & Automated Approval System (ACAAS)

Army Materiel Command (AMC) / TACOM Life Cycle Management Command (LCMC)

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: 12335 / DA194045
- ☐ **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 DMDC 12 DoD

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 TBD, status message provided by IMCO

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.

50 U.S.C. 401, Congressional declaration of purpose; 50 U.S.C. 435, Purposes; DoD 5200.2R, Department of Defense Personnel Security Program Regulation; DoD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 12333, United States Intelligence Activities; E.O. 12829, National Industrial Security Program; and E.O. 12968, Access to Classified Information; and E.O. 9397 (SSN), as amended.

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.

This application automates the new hire and account approval processes. The information collected will be used to verify background investigation in order to determine if the candidate meets the requirements to be offered a Federal employment position at the Detroit Arsenal. The application stores data and routes information to local security personnel for review and approval prior to a job offer being presented to a potential new government employee. The application also automates the approval process and tracks which users have access to the Detroit Arsenal Network and TACOM LCMC systems and applications.

This DCI utilizes the following PII: Full name, SSN, birth date, place of birth, personal cell phone number, home phone number, home address, personal email address, security clearance, veteran status, and retirement status. In certain situation, an SF86 is attached and contains in addition to those listed above: height, weight, hair color, eye color, home and work email addresses, passport, residence information, selective service record, relative information, foreign contacts, foreign activities (interests), foreign business, professional activities, and foreign government contacts, foreign travel, psychological and emotional health, illegal use of drugs or drug activity, use of alcohol, investigations and clearance records, use of information technology systems, non-criminal court actions, association records.

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

Every system has the potential for information to become compromised and accessible by individuals without an official need-to-know, whether through conventional hacking techniques, lost media, or intentionally by an insider. The system has implemented the latest cyber security safeguards to reduce an outside attack.

Every individual who has access to the system, with regards to using the entered data, has undergone a security background review and privacy and security training. The ACAAS data-at-rest is encrypted at the application level prior to being stored in an Application Infrastructure SQL database. Access to the application is limited to person(s) responsible for executing the new hire and out processing process(s). Data is backed up on the SQL database daily for reconstruction of the records should the system fail. Access to the server is Public Key Infrastructure (PKI) controlled.

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. TACOM Life Cycle Management Command (LCMC), Detroit Arsenal, Army Garrison, Tank Automotive Research Development and Engineering Center (TARDEC), Program Executive Office Ground Combat Systems (PEO GCS), Program Executive Office Combat Support & Combat Service Support (PEO CS&CSS) , Army Contracting Command - Warren (ACC-Warren)

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Civilian Personnel Advisory Center (CPAC)

☐ **State and Local Agencies.**

Specify.

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

Specify. Unified Business Technologies (UBT). "When on the Army Network the contractor shall store FOUO, Sensitive and Personally Identifiable Information (PII) on an encrypted drive or in an encrypted folder IAW Data at Rest (DAR) regulations and requirements within 10 days of availability. Information deemed as High Risk PII shall not be taken off the facility. If a critical mission need requires a contractor to take High Risk PII off the facility it shall be approved in writing from the COR and the Government organizations privacy coordinator. Examples of High Risk PII include Social Security Numbers, payroll information and personal medical information regarding someone other than you."

☐ **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.

Individuals may choose to not provide the information within USA Staffing prior to the application being submitted.

(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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Information is required for the completion of a background check prior to job offer.

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.

The following information will be presented to each individual via email when asked to provide PII data directly to ACAAS:

AUTHORITY: 50 U.S.C. 401, Congressional declaration of purpose; 50 U.S.C. 435, Purposes; DoD 5200.2R, Department of Defense Personnel Security Program Regulation; DoD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 12333, United States Intelligence Activities; E.O. 12829, National Industrial Security Program; and E.O. 12968, Access to Classified Information; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): The information collected will be used to verify background investigation in order to determine if the candidate meets the requirements to be offered a Federal employment position at the Detroit Arsenal and authenticate user request for access to the Detroit Arsenal Network.

ROUTINE USE(S): None. Data is not going to be used outside the Department of Defense.

DISCLOSURE: Voluntary. However failure to provide all required information would result in the candidate's application for hire to be rejected and/or access to the Detroit Arsenal Network denied.

Some information is obtained from the USA Staffing website, which provides the following Privacy Advisory:

YOUR PRIVACY IS PROTECTED

This information is used to determine if our equal employment opportunity efforts are reaching all segments of the population, consistent with Federal equal employment opportunity laws. Responses to these questions are voluntary. Your responses will not be shown to the panel rating the applications, to the official selecting an applicant for a position, or to anyone else who can affect your application. This form will not be placed in your Personnel file nor will it be provided to your supervisors in your employing office should you be hired. The aggregate information collected through this form will be kept private to the extent permitted by law. See the Privacy Act Statement below for more information.

Completion of this form is voluntary. No individual personnel selections are made based on this information. There will be no impact on your application if you choose not to answer any of these