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 AAFES 1703.03

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 24 JAN 2011
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.

The Privacy Act SORN (AAFES 1703.03) authorities include:

E.O. 12065

Army Regulation 215-4, Non-appropriated Fund Contracting

Army Regulation 60-20, Army and Air Force Exchange Service Operating Policies

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 will automate the current manual account approval process. This application tracks which users have access to TACOM LCMC systems and applications and provides a workflow to get that access granted in a timely fashion. Currently, some systems and applications have different approval chains and procedures, which is costly in time due to repeat requests for the same user information. The automated system will provide for a single point of entry for supervisors to request access to systems and applications for their personal, which includes approval and tracking by the TACOM LCMC G-2 for security clearance verification. The goal is to eliminate redundant requests for information, ensure accurate, one source tracking of access permissions for each user, and to complete the tracking cycle by automatically removing users from access when they no longer require it. This system will service Warren Detroit Arsenal users to include government, contractors and military personnel. The long term strategy will be to use this system at all TACOM LCMC depots and arsenals. The system will be built using the .net development environment and will use MICROSOFT SharePoint 2007 as the workflow engine. The current iteration of this system is the TACOM G-2 Security Roster. A second module is the CAC Kiosk which access the G2- Security Roster to verify clearances during meetings.

The type of PII collected is personal and employment.

G2 Security Roster is used to store approved employees based on security clearance that are located at the TACOM LCMC Detroit Arsenal. The security roster is also used for off site users that may require access to a System that is stored at TACOM LCMC Detroit Arsenal. These duties are official administrative duties that is performed by persons who have been properly screened and cleared for system need-to-know by G2.

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

The G2 administrators and the system owners receive initial and annual refresher Privacy Act and Information Assurance Training.

The G2 Security roster will be maintained in an encrypted Application Infrastructure SQL database. Access to the Security Roster is limited to person(s) responsible for updating the roster and granting access to a system or the operating system of the server. 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) Control.

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 LCMC Detroit Arsenal/ Army Garrison/ TARDEC/ Detroit Arsenal PEOs

☐ **Other DoD Components.**

Specify.

☐ **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.

A person trying to gain employment cannot object to the collection of PII because full name, SSN# and clearance type are required for employment. G2 administrators are the only individuals that can access PII information in the security roster.The SF86 form used in clearance investigation for employment states, "Giving us this information is voluntary. If you do not provide each item of requested information, however, we will not be able to complete your investigation, which will adversely affect your eligibility for a national security position."

(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 person trying to gain employment cannot object to the collection of PII because full name, SSN# and clearance type are required for employment. G2 administrators are the only individuals that can access PII information in the security roster. The SF86 form used in clearance investigation for employment states, "Giving us this information is voluntary. If you do not provide each item of requested information, however, we will not be able to complete your investigation, which will adversely affect your eligibility for a national security position."

(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.

SF 85 and SF 86 include the following language similar to a "Privacy Act Statement":

Purpose of this Form

The United States (U.S.) Government conducts background investigations and reinvestigations of persons under consideration for or retention in national security positions as defined in 5 CFR 732 and for positions requiring access to classified information under Executive Order 12968.
Withholding, misrepresenting, or falsifying information will have an impact on a security clearance, employment prospects, or job status, up to and including denial or revocation of your security clearance, or your removal and debarment from Federal Service.
This form is a permanent document that may be used as the basis for future investigations, security clearance determinations, and determinations of your suitability for employment. Your responses to this form may be compared with previous security questionnaires. It is imperative that the information provided be true and accurate to the best of your knowledge.

Authority to Request this Information

Depending upon the purpose of your investigation, the U.S. Government is authorized to ask for this information under Executive Orders 10450, 10865, 12333, and 12968; sections 3301, 3302, and 9101 of title 5, U.S. Code (U.S.C.); sections 2165 and 2201 of title 42, U.S.C.; chapter 23 of title 50, U.S.C.; and parts 2, 5, 731, 732, and 736 of title 5, Code of Federal Regulations.
Your Social Security Number (SSN) is needed to identify your unique records. Although disclosure of your SSN is not mandatory, failure to disclose your SSN may prevent or delay the processing of your background investigation. The authority for soliciting and verifying your SSN is Executive Order 9397.

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.