PRIVACY IMPACT ASSESSMENT (PIA)

For the

GFIS - G8 Financial Information System
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: 10577 / DA182765
- ☐ **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 T7335a

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. 301, Departmental Regulations; Chapter 53, Pay Rates and Systems, Chapter 55, Pay Administration, Chapter 61, Hours of Work and Chapter 63, Leave; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 8, Chapter 5, Leave; 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.

ATAAPS Utility Reports and Forms is a module within the G8 Financial Information System. It is used by G-Staff ATAAPS Administrators to retrieve reports from the ATAAPS Oracle database in Oklahoma to help maintain it, troubleshoot problems and to verify SDA file creation. Forms necessary to process ATAAPS actions are provided through the web interface. It is used by payroll CSR to troubleshoot payroll issues. It is used by Internal Review for team and roster report verification during audits. It is used by LMP financial analysts for troubleshooting LMP Labor cost issues.

PII utilized includes: full name, SSN, EDIPI, Active Directory ID, Employment Information (time and attendance)

(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 and lower the risk of lost electronic media. 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.

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. Army Audit Agency (AAA), Army Contracting Command (ACC), Army Materiel Command (AMC), Department of the Army Inspector General, Department of the Army's Office of the Assistant G-1 for Civilian Personnel (AG-1 CP), Installation Management Command (IMCOM), Intelligence and Security Command (INSCOM), Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA/ALT), Office of the Assistant Secretary of the Army for Financial Management and Comptroller (ASA/FMC), TACOM Life Cycle Management Command (LCMC), United States Army Criminal Investigative Command (CID), and Department of Army (DA)

☒ **Other DoD Components.**

Specify. Department of Defense (DOD) Inspector General, Defense Criminal Investigative Service (DCIS), Defense Finance and Accounting Service (DFAS), Defense Information Systems Agency (DISA)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

Information is not shared with contractors outside of the organization. However, Database administrators are contractors under this contract:

UBT Contract W56HZV-11-D-L555 Section C. 1.4.9.2 describes requirements for data-at-rest (DAR) and high-risk PII; Section C.1.10 describes security risks, enforces adherence to the Privacy Act of 1974, and lists the contractor as the responsible entity.

The following language in their contract to safeguard PII:

"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.

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

Individuals do not use this application. End users are comprised of organization time keepers, payroll representatives, and financial analysts, and they do not enter PII into the system. PII is collected from multiple DoD/Army systems and the individual would have to object within those system. However, Army pay and personnel systems still rely on SSN to uniquely identify the employee and there is no way for an employee to reject to this use. SSN is used within the system to uniquely identify the employee and data match with the systems listed in Section 3.a(2).

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.

SSN is used by Army payroll and personnel systems to uniquely identify the individual. PII is collected from multiple DoD/Army systems and is provided as reports and data feeds from those systems. Information is only used to facilitate mission requirements. Information is not collected directly from the individual therefore they have no opportunity to consent to the use of the PII. Information is necessary for normal administration of employee and payroll actions, and would be required even if this system did not exist. This system replaces a manual process that would involve excel spreadsheets and emails.

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 PII and are not involved in the collection information. The average individual would not even be aware of the application. External to this system, individuals are provided notice of SSN usage when they become Department of the Army civilians, and notified that their SSN will be used to uniquely identify them within Army systems.