PRIVACY IMPACT ASSESSMENT (PIA)

For the

PEO GCS KNOWLEDGE CENTER PORTAL

ASA(ALT) - Program Executive Office (PEO) Ground Combat Systems (GCS)

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: 3743/ DA76303
- ☐ **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 A0025-1 CIO G6

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.

DoD 1100.4 Guidance for Manpower Management
AR 570-4 Manpower and Equipment Control, Manpower Management
AR 570–5 Manpower Staffing Standards System
DoD Directive 1100.4 Guidance for Manpower Programs
DoD 5010.15.1-M Standardization of Work Measurement
DoD Instruction 5010.39 Productivity Enhancing Capital Investment

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 PEO GCS KNOWLEDGE CENTER PORTAL integrates a Enterprise Personnel Database (ePDB) as a strategic planning tool which provides a means to manage PEO GCS human capital and associated manning information. ePDB consolidates data from two standard Army applications Defense Civilian Personnel Data System (DCPDS) and Career Acquisition Management Portal (CAMP), SORN # A0025-1 CIO G6, and incorporates manpower standards and manpower requirements criteria (requirements and authorizations) to support the overall manpower management process by providing a credible basis for manpower and budget requests. ePDB is a strategic planning tool that takes into account the current workforce capacity, required skills and other factors, resulting in workforce reporting and analysis that promotes organizational long-term goals. ePDB collects names, email address, birthdays, work address, emergency POC name and number, home address, nick name, and rank.

The Advanced COOP Personnel Database (ACPD) is used for personnel accountability requirements for the organization. The ACPD collects names, personal cell phone, home phone, work phone, work email, and/or personal email.

The Program Management Offices utilize a Personnel List which is used for Human Resources collaboration purposes. This list is used to track employee records on any change of status within the organization. This list tracks name, suborganization, location, position, work phone, cell phone, email, CAC ID, birthday, travel credit card, rank, service comp day/year, address, emergency POC/phone, retirement/reassignment date.

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

Privacy risks associated with the PEO GCS KNOWLEDGE CENTER PORTAL integrated with Enterprise Personnel Database (ePDB), Advanced COOP Personnel Database (ACPD), and Personnel List are low-impact. Limited linkable personally identifiable information (PII) will be collected only as it relates to existing career information. Risks will be mitigated by requiring CAC authentication, password access, field level data encryption, and user-based security role access. Additionally, data is accessible by a limited number of Army employees, all whom have security clearances. Data is read-only and shared over a secure network.

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. U.S. Army organizations only; PEO GCS, TACOM Life Cycle Management Command (LCMC), PEO CS&CSS, TARDEC, ACC-WRN

☐ **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.

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

New PII is not collected by PEO GCS KNOWLEDGE CENTER PORTAL, data is consolidated from two existing standard Army systems, CAMP (SORN # A0025-1 CIO G6), is only consolidated and integrated into a Enterprise Personnel Database (ePDB), Advanced COOP Personnel Database (ACPD), and Personnel List which is hosted within the PEO GCS KNOWLEDGE CENTER PORTAL. This information is required in order to provide workforce capacity planning for senior leaders, and COOP purposes.

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.

New PII is not collected by the PEO GCS KNOWLEDGE CENTER PORTAL, data is consolidated from two existing standard Army systems, CAMP (SORN # A0025-1 CIO G6) & DCPDS, is only consolidated and

integrated into a Enterprise Personnel Database (ePDB), Advanced COOP Personnel Database (ACPD), and Personnel List which is hosted within the PEO GCS KNOWLEDGE CENTER PORTAL. This information is required in order to provide workforce capacity planning for senior leaders, and for COOP purposes.

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.

Privacy Advisory will read as follows; "This application will display Personally Identifiable Information (PII). Please control displays and printouts in accordance with the local policy and in ways that deter unauthorized individuals from reading the information."

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.