PRIVACY IMPACT ASSESSMENT (PIA)

For the

UPDB - USAREUR PERSONNEL DATABASE (EUR)

US ARMY in Europe HQ (HQ USAREUR)

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: 4069 DA01136
- ☐ **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 A0600-8-104

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://dpcld.defense.gov/Privacy/SORNs.aspx

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.

Following are legal references that justifies use of the SSN in the UPDB system
10 U.S.C. 3013, Secretary of the Army Army Regulation 600–8, Military Personnel Management E.O. 9397 (SSN) , as amended
AR 55-46, Travel Oversees, 20 Jun 1994
AR 614-30, Overseas Service, 22 Dec 2016
AR 614-200 Enlisted Assignments, 26 Feb 2009

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 USAREUR Personnel Database (UPDB), provides web-based automated tools for over 1500 users in the European Theater, and thousands of Soldiers world-wide in these critical mission areas; European Theater Readiness Management, Reception Center Processing, VIPER Theater Report Tool, Theater Transformation, Family Travel`, Student Travel, and a number of theater-wide missions that use the custom data services provided by UPDB; e.g., Central Tasking Branch, 7th Army Training Command, Community Housing, Community In-processing, and Vehicle Registration.

Theater human resource (HR) managers, who service a large population of Soldiers either in Europe or on orders to Europe, rely on UPDB automation tools, data, and Web applications to support Theater unique business processes. Should UPDB fail, HR managers will struggle to meet mission requirements using DA automation systems (eMILPO, EDAS, TOPMIS I & II, Web-TAADS, etc) that only partially support Theater unique business processes. UPDB must remain a viable system until a future DA HR System implementation absorbs all critical UPDB functionality, or it has been determined that UPDB functionality is no longer needed; letting UPDB fail before this critical juncture will result in a significant negative impact on Theater HR operations.

UPDB collects Soldier Personally identifiable information required to manage Soldier assignments and Soldier HR functions in the USAREUR Theater.

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

UPDB privacy risks associated with the PII collected is managed through the application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) process. RMF security controls are regularly validated on a continuous and ongoing basis to ensure that all required enterprise system safeguards are in place to protect PII data; annual training is conducted to ensure that UPDB personnel are cognizant of the PII data protection responsibilities, and PII data handling statements are reviewed and acknowledged by all UPDB users monthly.

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. DOA

☐ **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.

Click through statement that informs user of data collection. User can opt out of data collection but will not be able to utilize the UPDB system.

(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.

PII collected is FOUO and is disseminated to vetted HR managers with "need to know". PII is collected from Department of the Army HR systems and is needed for the day to day support of the Army in Europe military human resource mission.

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.

Authority: See section 2.f

Principal Purpose(s): See section 2.g.(1)

Routine Use(s):

Law Enforcement (Investigations): To the appropriate federal, state, local, territorial, tribal, or foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

Department of Justice for Litigation: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

Breach Mitigation and Notification: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Breach Mitigation and Notification: To another Federal agency or Federal entity, when the Department of Defense (DoD) determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosure: Voluntary. However, failure to provide information may result in denial of access.