PRIVACY IMPACT ASSESSMENT (PIA)

For the

VERINET - VEHICLE REGISTRY INQUIRY NETWORK (EUR)

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: 4084 DA01146
- ☐ **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 A0190-5 OPMG

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.

U.S.C. 301, Departmental Regulations; 10 U.S.C 3013, Secretary of the Army and E.0. 9397 (SSN), A0190-5 OPMG

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.

VERINET is the mission essential automated system for law enforcement and security forces used to register privately owned vehicles and firearms, as well as the issuance and control of drivers licenses for all U.S. Forces personnel in Germany. The system provides 24-hour a day notifications to the German authorities required by Articles 9 -11 of the Supplementary Agreement to the NATO Status of Forces Agreement and other memorandums of agreement with the Federal Republic of Germany. It is also used as an adjunct system for HQ USAREUR for law enforcement and force protection to identify all vehicles and license plates, including stolen and lost vehicles and license plates, to ensure positive identification, use, and access to installations throughout the command and to preclude or mitigate illegal use or access to all installations in Germany.

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

The primary risk to PII is theft. PII data is encrypted at rest using EFS or BitLocker, and during transmit using PKI encryption and Secure File Transfer Protocol (SFTP). PII user education exists and is refreshed annually.

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. US Forces and Host Nation law enforcement authorities

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. US Department of State (Criminal Intelligence-related information) & FBI

☐ **State and Local Agencies.**

Specify.

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

Specify. Limited to contracting officer representative and contracting technical officer representative.

☐ **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.

Privacy act statements are required on all pertinent actions. A warning disclaimer is included in the statement. All network users are required to read and sign an "Acceptable Use Policy (AUP)" before permitting them access to USAREUR NIPRNet. Individuals have an option to decline. However, doing so will prohibit the person's access to the network. Additionally, the U.S. Government uses SF 86: (Questionnaire for National Security Positions) to conduct background investigations and re-investigations on persons under consideration for or retention in national security positions, and for positions requiring access to classified information. The SF86 specifically states: "Giving us this information is voluntary. If you do not provide an item of the 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.

Privacy act statements are required on all pertinent actions. A warning disclaimer is included within the statement. All computer users are required to read, and sign an Acceptable Use Policy (AUP) in order to obtain approval for access to USAREUR NIPRNet. Computer users have an option to decline, but doing so will prevent the person from obtaining access to the network. Yes, please see section 2(i)(1), pertaining to the use of SF 86,

(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.

Applicants are immediately presented with a statement on the front page of SF86 (Questionnaire for National Security Positions), which explains the purpose of the form; why the information must be provided and the ramifications for failing to do so.

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.