PRIVACY IMPACT ASSESSMENT (PIA)

For the

REAL ESTATE KNOWLEDGE MANAGEMENT SYSTEM (REKMS)
US Army Corps of Engineers

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 DA308023

☐ **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

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.

PUB L. 104-106 (110, Stat 186, Section 2801. National Defense Authorization Act for Fiscal Year 1996

10 U.S.C. §§ 2871 et seq, 10 U.S.C. § 2872, 10 U.S.C. § 2872a, 10 U.S.C. § 2873
10 U.S.C. § 2874, 10 U.S.C. § 2875, 10 U.S.C. § 2876, 10 U.S.C. § 2877,
10 U.S.C. § 2878, 10 U.S.C. § 2880, 10 U.S.C. § 2881, 10 U.S.C. § 2881a
10 U.S.C. § 2882, 10 U.S.C. § 2883, 10 U.S.C. § 2883a, 10 U.S.C. § 2884
10 U.S.C. § 2885

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 Army has instituted multiple programs to privatize a variety of real property assets, and is responsible for the management and oversight of these assets. To support the U.S. Army Corps of Engineers (USACE) Norfolk District's (NAO) mission to manage the massive long-term storage requirement of the Residential Communities Initiative (RCI), Privatization of Army Lodging (PAL) and Unaccompanied Personnel Housing (UPH) programs, USACE NAO has implemented the Real Estate Knowledge Management System (REKMS), a document management system using the OpenText Documentum Enterprise Content Management System (CMS), associated Content Intelligence Services (CIS), and Captiva scanning solution used to capture, store, manage, search and retrieve electronic documents. Program stakeholders at Assistant Secretary of the Army (Installations, Energy and Environments) ASA (IE&E), Office of the Assistant Chief of Staff for Installation Management (OACSIM), Installation Management Command (IMCOM), USACE and others Department of Defense (DoD) organizations on an as needed basis.

Program documents are imported, scanned and indexed by the programs administrators. Documents can be searched, viewed, and downloaded by program stakeholders.
PII collected includes the First and Last Name, Installation Name, Work Phone Number, DOD ID number, and Official E-Mail Address of RCI/UPH team members. This information is used to grant access to the system which does not contain PII.

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

It is possible that a user may inadvertently or intentionally disclose PII to an unauthorized user. Users are required to take annual IA training as referenced in DoDI 8500.2. Role-based security is in place to allow only appropriate application/system administrator users access to the data. Users not associated with application/system administrator can not access the data. Risks regarding the collection, use and sharing of PII in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls. Specifically, these risks are addressed by protecting the data collection resource with strong SSL encryption, programmatically restricting the system from releasing PII data through its interfaces, through access control restricted by CAC to internal network personnel whose job functions require access to PII.

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 Civilians

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.