



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Housing Operations and Management System Version 4 (HOMES4)

OACSIM

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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.

10 U.S.C. 3013, Secretary of the Army; Pub.L. 104-106, Military Housing Privatization Initiative (MHPI) Act of 1996; DoD Directive 4165.63, DoD Housing; Army Regulation 210-50, Housing Management; 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.

HOMES4 is a COTS web-based system that replaces the HOMES3 client-server system. HOMES is an installation-level housing operations management system that supports the housing counselors providing on-post government housing, off-post housing, unaccompanied personnel housing (UPH) and furnishings management. The system provides housing management statistical data and reports to the installation, tenant commands, IMCOM, and HQ DA. This system will no longer be used as of 29 Sep 2011.

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

Records are maintained in areas accessible only to authorized persons having official need. Records are housed in buildings protected by security guards or locked when not in use. Information in automated media is further protected by physical security devices; access to or update of information in the system is protected through a system of passwords and usage of the Common Access Cards (CACs), thereby preserving integrity of data. RETENTION AND DISPOSAL: Army Family Housing, Unaccompanied Personnel Housing and Off-Post housing files are destroyed after 3 years; installation housing project tenancy files are destroyed 3 years after termination of quarters occupancy; family housing leasing files are destroyed 3 years after lease terminates is canceled, lapses, or after any litigation is concluded; housing, facility and complaint records are destroyed after 10 years; housing referral services are destroyed after 5 years; off-post rental housing reports are destroyed after 2 years; and off-post housing complaints and investigation are destroyed 10 years after completion at office; Army-wide responsibility.

**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. All Army Installation and tenant commands, Army Installation Management Command, and Head Quarters Department of Army

**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.

The Army's rules for accessing records, and for contesting contents and appealing initial agency determinations are contained in Army Regulation 340-21; 32 CFR part 505; or may be obtained from the system manager. Preventing collection of their PII would prevent the Soldier from completing their housing applications to receive Government Housing.

(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.

The soldier will provide his information for the purpose of obtaining Government Housing. If the Soldier decides to withhold his/her information they will not be allowed to continue their application to apply for Government Housing. By not providing their consent, they are refusing to accept or apply for housing.

(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.

The FOUO statement is used in the HOMES4 System. 5 U.S.C, 552a(b) of the Privacy Act is referenced and acknowledges that these records or information contained therein may specifically be disclosed outside the DOD as a routine use to 5 U.S.C. 552a(b) 3.

To assign soldiers to housing units in accordance with BAH rates/eligibility. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the Department of Housing and Urban Development to resolve and/or adjudicate matters falling within their jurisdiction. To the Residential Community Initiatives (RCI), a private non-governmental entity, to execute the privatization of residential communities for Soldiers and their families under the authority of Military Housing Privatization Initiative (MHPI) Act of 1996. The 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.

**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.**