U.S. DEPARTMENT OF HOUSING AND URBAN DEVLEOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
"INVENTORY MANAGEMENT"
(OMB Unique Identifier 025000106010000000301093 and PCAS # 01667960)
November 2004

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Advocate's determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- Privacy Act of 1974, as amended affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See http://www.usdoj.gov/foia/privstat.htm; see also HUD Handbook1325.1 at www.hudclips.org);
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See http://www.usdoj.gov/foia/privstat.htm);
- Freedom of Information Act of 1966, as amended (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also HUD's Freedom of Information Act Handbook (HUD Handbook 1327.1 at www.hudclips.org);
- E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- Federal Information Security Management Act of 2002 (which superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at Title 44 U.S. Code chapter 35 subchapter II (http://uscode.house.gov/search/criteria.php); and
- OMB Circular A-130, Management of Federal Information Resources, Appendix I (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those HUD staff who have been authorized because of their duties; and they will be held accountable for ensuring privacy and confidentiality.

What is the Privacy Impact Assessment (PIA) Process?
The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?
Both the program area system owner and IT project leader work together to complete the PIA. The system owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT project leader describes whether technical implementation of the system owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

1. New Systems: Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).

2. Existing Systems: Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA): Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

Privacy Act. The Privacy Act of 1974, as amended (http://www.usdoj.gov/foia/privstat.htm) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Publication of PIA summary. The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD’s Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD’s web site. See: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Advocate in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A) for that question, and briefly explain why it is not applicable.

Program Area: Office of Public and Indian Housing – Real Estate Assessment Center (REAC)
Subject matter expert in the program area:
Program area manager: Elizabeth Hanson, Director, Real Estate Assessment Center, 202-708-4932 Ext. 3328
IT Project Leader: Charles D. "Dave" Moore (PIH's Information Services Division) 202-708-1445 ext. 4158; and Jim Williams (PIH's Information Services Division, 202-708-0614 ext. 3442)

For IT Systems:

- **Name of system:** Inventory Management
- **PCAS #:** 01667960
- **OMB Unique Project Identifier #:** 02500010601000000301093

For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

Question 1: Provide a brief description of what information is collected, and why.
The Public and Indian Housing Information Center (PIC) system had a preliminary PIA conducted in 2003. PIC is being realigned to meet future state architecture requirements; most of the current PIC data will be contained in the Inventory Management system.

The system will provide the basic foundation to achieve the Departmental goals to assure that grantees receive the dollars needed to provide safe and decent housing and related community and economic services to residents and communities across the nation. The initiative provides the automated capture and management of core data required to assure that grantees receive the formula and categorical grant program funds appropriated by Congress for Public Housing Capital Fund, Public Housing Operating Subsidy Fund, Section 8 Housing Choice Vouchers, Native American Housing, and Resident Opportunities and Self-Sufficiency program.

The Inventory Management system will provide a central data repository for information about the public housing inventory, PIH business events, and PIH program areas.

It will also contain personal information about the residents of the public housing units – extracted from the HUD 50059 form, and detailed in the chart below.

The system will interface with:

- HUD's Line of Credit Control System (LOCCS) for funds balance status;
- Personnel Information System (PERIS) for security access checking;

- HUD’s Central Accounting and Program System (HUDCAPS) for transaction-level accounting information;
- Physical Assessment Sub-system (PASS) for ratings of the physical condition of PHA-run properties;
- PIH’s future Resource Allocation tool for tracking funds allocated to the PHA; and
- PIH’s future Oversight and Monitoring system for leasing, vacancy rate, and expense data.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

X	Name
X	Social Security Number (SSN)
X	Other identification number (specify type): Alien Registration Number
X	Birth date
X	Home address
	Home telephone
	Personal e-mail address
	Fingerprint/ other “biometric”
	Other (specify):
	None

Personal/ Sensitive Information:

X	Race/ ethnicity
	Marital status
X	Gender/ sex
X	Spouse name
X	# of children
X	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
	Employment history
	Education level
	Medical history/ information
X	Disability
	Criminal record
	Other (specify):
	None

Question 2: Type of electronic system or information collection. Fill out Section A, B, or C as applicable.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

X	Yes
	No

NOTE: PIC is being realigned to meet future state architecture requirements; most of the current PIC data will be contained in the Inventory Management system, being developed starting in FY 2005.

B. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

	Conversion: When paper-based records that contain personal information are converted to an electronic system
	From Anonymous (Non-Identifiable) to "Non-Anonymous" (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
X	**Significant System Management Changes:** When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new "relational" databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
X	**Merging Databases:** When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
	New Public Access: When new public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
X	**New Inter-agency Uses:** When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
X	**Business Process Re-engineering:** When altering a business process results in significant new uses, disclosures, or additions of personal data
X	**Alteration in Character of Data:** When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

C. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.

	Yes, this is a new ICR and the data will be automated
	No, the ICR does not require a PIA because it is not new or automated)
X	N/A
	Comment:

Question 3: Why is the personally identifiable information being collected? How will it be used? Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

Rental Housing Assistance:

X	Eligibility for rental assistance or other HUD program benefits
X	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
X	Property inventory (address of development, number of apartment units, etc.)
X	Property inspections
	Other (specify):
	Comment:

Grants:

X	Grant application scoring and selection – if any personal information on the grantee is included
X	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
X	Comment: The only “personal” information collected on grantees relates to their business contact information.

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

	Employee payroll or personnel records
	Payment for employee travel expenses

	Payment for services or products (to contractors) – if any personal information on the payee is included
X	Computer security files – with personal information in the database, collected in order to issue user IDs
	Other (specify):
X	Comment: User name, organization, and SSN are collected in order to issue user IDs.

Other lines of business (specify uses):

Question 4: Will you share the <u>personally identifiable</u> information with others (e.g., another agency for a programmatic purpose, or outside the government)? Mark any that apply:

X	Federal agencies? (specify):
X	State, local, or tribal governments?
X	Public Housing Agencies (PHAs) or Section 8 property owners/agents? NOTE: PHAs will submit inventory management data to HUD via a secure web site. Any information shared back with the PHAs will pertain only to that PHA's operations, not other PHA's operations.
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):

Question 5: Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

X	Yes, they can "opt-out" by declining to provide private information or by consenting only to particular use
	No, they can't "opt-out" – all personal information is required

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): Declining to provide information such as a SSN will result in no housing related grant, subsidy, or financial assistance being provided to the individual in question.

Question 6: How will the privacy of the personally identifiable information be protected/ secured? What are the administrative and technological controls? Mark any that apply and give details if requested:

X	System users must log-in with a password
X X	When an employee leaves: • How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? ____ PIH-REAC follows the HUD's policies and procedures for hiring, transferring, and termination of employees. Procedures are identified in HUD Security Program Policy Handbook, Section 4.3.2.1 and the WASS Security Plan 2004. • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): User access to PIC-REAC systems is controlled through the PIH-REAC roll on and roll off process. Additional application layer security is provided via unique user IDs and passwords given when establishing an account through WASS. Procedures are identified in HUD Security Program Policy Handbook, 4.3.12.1 and the WASS Security Plan 2004.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: • Full access rights to all data in the system (specify #)? Over 10 • Limited/ restricted access rights to only selected data (specify #)? 20-100
X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve): This control area is maintained by ISG.
X	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: Please see the PIC Security Plan for details.
	Other methods of protecting privacy (specify):
X	Comment: Users are granted different levels of access to the data, based on authorized need.

Question 7: If private information is involved, by what data elements can it be retrieved? Mark any that apply:

X	Name
X	Social Security Number (SSN)
X	Identification number (specify type): Alien Registration Number
X	Birth date
X	Race/ ethnicity
	Marital status
X	Spouse name
X	Home address

	Home telephone
	Personal e-mail address
	Other (specify):
	None

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

HUD's Public and Indian Housing Information Center (PIC) system had a PIA conducted in 2003. PIC is being divided into four separate systems, one of which is the proposed Inventory Management system.

The personal and sensitive data listed in Question 1 above is collected for the 2 million households receiving rental assistance each year under the programs administered by the Office of Public and Indian Housing (PIH). While Inventory Management will be a new system, the existing PIC system has a comprehensive Security Plan and strict access controls are in place, as summarized in Question 6 above. Also, the legislatively mandated program has been in existence for over 20 years, and the business process for re-certifying the eligibility of recipients is well-established.

Because of the vast amount of personal and sensitive information, we will annually monitor this system and related business processes to ensure that adequate privacy protections continue to be in place.

__/signed/____________________________	November 8, 2004
Eric M. Stout	date
Privacy Advocate, Office of the Chief Information Officer	
U.S. Department of Housing and Urban Development	