

U.S. Department of Housing and Urban Development

Public and Indian Housing Real Estate Assessment Center Information Technology Division

Inventory Management System (IMS)

Formerly the Public and Indian Housing
Information Center – PIC)

Privacy Impact Assessment

August 2008

Document Endorsement

I have carefully assessed the Privacy Impact Assessment (PIA) for **Inventory Management System**. This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

PLEASE CHECK THE APPROPRIATE STATEMENT.

X **THE DOCUMENT IS ACCEPTED.**
 THE DOCUMENT IS ACCEPTED PENDING THE
 CHANGES NOTED.

Based on our authority and judgment, the data captured in this document is current and accurate.

/S/ Elizabeth Hanson

Elizabeth Hanson, System Owner
PIH- Real Estate Assessment Center

8/28/08

Date

/S/ Hitesh Doshi

Hitesh Doshi, IMS System Project Manager
PIH-REAC-IT DIVISION

08/28/08

Date

N/A

Departmental Privacy Advocate
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

Date

/S/ Donna Robinson Staton

Donna Robinson Staton, Departmental Privacy Act
Officer

Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

09/09/08

Date

Table of Contents

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	5
Why is the PIA Summary Made Publicly Available?	5
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT.....	7
Question 1: Provide a brief description of what personal information is collected.	7
Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?	8
Question 3: Type of electronic system or information collection.....	10
Question 4: Why is the personally identifiable information being collected? How will it be used?	12
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	13
Question 6: 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)?	
Question 7: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	13
Question 8: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	14
SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....	15

FINAL/APPROVED

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA)**

“INVENTORY MANAGEMENT SYSTEM”

OMB Unique Identifier#: 02500010601000000301093

PCAS # 001667960

August 2008

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 Handbook 1325.1 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 superseded 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 that are 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

Program Area: Office of Public and Indian Housing – Real Estate Assessment Center (REAC)

Subject matter expert in the program area: Robert Dalzell, PUBLIC HOUSING REVITALIZATION SPECIALIST, CAPITAL PROGRAM DIVISION. PIH/REAC, (202) 402-4216

Program area manager: Elizabeth Hanson, Director, Real Estate Assessment Center, (202) 475-7949

IMS IT Project Leaders:

1. Hitesh Doshi, IMS Government Technical Monitor, PIH-REAC-IT Division, (202) 475-8940

2. Yvette Connor, Government Technical Representative, OCIO Contract Oversight Division, PIH/REAC IT Projects/Contracts

3. Dudley Ives, IMS Alternate GTM, and GTM for the Disaster Information System, PIH-REAC-IT Division, (202) 475-8603

For IT Systems:

Name of system: Inventory Management System

PCAS #: 001667960

OMB Unique Project Identifier #: 02500010601000000301093

For Information Collection Requests:

Name of Information Collection Request: Family Report, Moving to Work (MTW) Family Report

OMB Control #: OMB approval number is 2577-0083, expiration date 3/31/2010

Question 1: Provide a brief description of what information is collected, and why.

The Office of Public and Indian Housing's, Inventory Management System (IMS), conducted its preliminary PIA in April 2003 and it was updated during November 2004. The purpose of this update is to evaluate the current processes to ensure that adequate protection of the personal data collected by IMS.

The system provides 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, and Section 8 Housing Choice Vouchers.

In Addition, the Inventory Management System provides a central data repository for information about the public housing inventory, PIH business events, and PIH program areas.

IMS contains personal information about the residents of the public housing units – extracted from the form HUD 50058 as detailed in the charts 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: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

What security controls are in place to protect the information (e.g., encryptions)?

The IM System makes use of a distributed, role-based user creation and access level system that restricts users' access by both sensitivity level and geographic region. As an example, this system prevents a Boston Public Housing Authority user from submitting, modifying, or viewing data affecting the New York Public Housing Authority regardless of their level of access for Boston PHA data. Policies and procedures exist governing the requesting, establishing, issuing and retiring of user accounts. The user account request process will be extended such that the requesting individual must read, agree to abide by, sign and return a copy of the Rules of Behavior.

For IMS application access PIH-REAC requires users to use the single sign-on security interface WASS (Web Access Security System). WASS consists of a secure connection component and a secure systems component. They provide an overall security umbrella for thousands of HUD-wide system users. The secure connection component of WASS includes online registration forms that are accessible via the World Wide Web and are used by HUD's trusted Business Partners to submit requests for the authority to access secure systems that reside behind HUD's firewall. The data captured by the secure connection registration pages is used to establish authorized users on the Lightweight Directory Access Protocol (LDAP) server. Secure Connection provides system level security by validating users against the LDAP server prior to providing them access to HUD's Secure Systems environment from the Internet. Users are validated by capturing their user identifications (IDs) via the authentication box that is displayed upon connection to the LDAP server. Upon a user's valid entry into HUD's secure systems environment, control is passed from secure connection to secure systems, which enforces application security.

What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?

VPN

Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department?

YES

Is there a policy that identifies “if” or “if not” downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Policy permits remote access, but prohibit downloading and local storage.

Comment: The focus of information security is on ensuring protection of information and continuation of PIH operations. Providing efficient accessibility to necessary information is the motivation for establishing and maintaining automated information systems. For the IMS, there are controls in place to restrict IMS output. The controls include:

- Physical protection of information processing facilities and equipment.
- Maintenance of application and data integrity.
- Assurance that automated information systems perform their critical functions correctly, in a timely manner and under adequate controls.
- Protections against unauthorized disclosure of information.
- Assurance of the continued availability of reliable and critical information.

The HUD PIH IMS System Administration Guide provides operational guidance to the HUD Information Technology organization and facilitates the deployment, maintenance, backup and monitoring of the IMS infrastructure. This document provides both general and detailed procedures related to IMS system administration.

Protection Procedures

Procedures to ensure unauthorized individuals cannot read, copy, alter or steal printed and electronic information are the following:

- Procedures are in place to insure that all users handle both the display of sensitive information via the web interface and any hardcopies of such data in a responsible and secure manner. Hardcopies of data, such as printouts of IMS System information displays or reports that are no longer needed are to be shredded and disposed of.
- Processing of sensitive information is maintained in controlled areas of the facility.
- Hardware inventory is managed via inventory lists and audit trails for transported equipment.

Question 3: Type of electronic system or information collection.

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)?

	Yes	No
If yes, please proceed to answering the following questions.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Does the system require authentication?	<input type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input type="checkbox"/>

A. 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):

X	Conversion: When paper-based records that contain personal information are converted to an electronic system form HUD 50058
N/A	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
N/A	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)
N/A	New Public Access: When <u>new</u> 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)
N/A	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
N/A	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
N/A	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)

B. 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.

C.

	Yes, this is a new ICR and the data will be automated
	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
	N/A
X	Comment: ICR needed to obtain approval from OMB for HUD form 50058.

Question 4: 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: None

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: None

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment: None

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):
	Comment: None

Other lines of business (specify uses):

	None
--	------

Question 5: Will you share the personally identifiable information with others (e.g., another agency for a programmatic purpose, or outside the government)? Mark any that apply:

<input checked="" type="checkbox"/>	Federal agencies? (SSA and HHS)
<input checked="" type="checkbox"/>	State, local, or tribal governments?
<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	FHA-approved lenders?
<input type="checkbox"/>	Credit bureaus?
<input type="checkbox"/>	Local and national organizations?
<input type="checkbox"/>	Non-profits?
<input type="checkbox"/>	Faith-based organizations?
<input type="checkbox"/>	Builders/ developers?
<input type="checkbox"/>	Others? (specify): None

Question 6: 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)?

<input checked="" type="checkbox"/>	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
<input type="checkbox"/>	No, they can't “opt-out” – all personal information is required

"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 7: 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:

<input checked="" type="checkbox"/>	System users must log-in with a password
<input checked="" type="checkbox"/>	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. PIH-REAC terminates the user ID simultaneously as the Employee ID is de-activated in HUD's Active ID Directory. How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve):

	There is an application layer of security that 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. PIH-REAC terminates the user ID simultaneously as the Employee ID is de-activated in HUD's Active ID Directory.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: <ul style="list-style-type: none"> • Full access rights to all data in the system (specify #)? 104 Active users. • 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 Internet Services Group (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: The protocol for sharing of data with the Enterprise Income Verification System (EIV) and the responsibility for protecting the privacy of data are identical as both systems (IMS and EIV) are maintained by the PIH-REAC-IT Division via the WASS system.
	Other methods of protecting privacy (specify):
X	Comment: Users are granted different levels of access to the data, based on authorized need.

Question 8: If private information is involved, by what data elements is it retrieved? Mark any that apply:

	Name
X	Social Security Number (SSN)
	Identification number (specify type): Alien Registration Number
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify): None

Other Comments (or details on any Question above): None

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

HUD's Public and Indian Housing Information Management System had a PIA conducted in 2003 and it was updated during 2004.

The personal and sensitive data listed in Question 1 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 System is the new name for PIC-Public and Indian Housing Information System, the existing system has a comprehensive Security Plan and strict access controls are in place, as summarized in Question 6. 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.