

# **U.S. Department of Housing and Urban Development**

---

## **Office of Single Family Housing**

### **Asset Disposition and Management System (ADAMS/P260)**

Privacy Impact Assessment

**September 2008**

## DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Asset Disposition and 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.

- The document is accepted.**  
 **The document is accepted pending the changes noted.**  
 **The document is not accepted.**

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

/s/ Vance Morris

**SYSTEM OWNER**  
**VANCE MORRIS, DIRECTOR, OFFICE OF**  
**SINGLE FAMILY ASSET MANAGEMENT**

9/23/08

**Date**

/s/ Ivery Himes

**PROGRAM AREA MANAGER**  
**IVERY HIMES, DIRECTOR, SINGLE FAMILY**  
**ASSET MANAGEMENT DIVISION**

9/23/08

**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

**DEPARTMENTAL PRIVACY ACT OFFICER**  
Office of the Chief Information Officer  
U. S. Department of Housing and Urban Development

9/23/08

**Date**

## TABLE OF CONTENTS

<b>DOCUMENT ENDORSEMENT .....</b>	<b>2</b>
<b>ENDORSEMENT SECTION .....</b>	<b>2</b>
<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>SECTION 1: BACKGROUND.....</b>	<b>4</b>
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?.....	6
Why is the PIA Summary Made Publicly Available? .....	6
<b>SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT.....</b>	<b>7</b>
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? .....	9
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)? .....	13
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	14
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	14
<b>SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....</b>	<b>15</b>

## **FINAL/APPROVED**

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

**ASSET DISPOSITION AND MANAGEMENT SYSTEM (ADAMS/P260)**

**OMB Unique Identifier #: for IT Systems: n/a  
and PCAS #: n/a – not WC funded**

**September 2008**

**NOTE:** See Section 2 for PIA answers, and Section 3 for Privacy Act Officer'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 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](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](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](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 \(http://uscode.house.gov/search/criteria.php\)](http://uscode.house.gov/search/criteria.php); and

- [OMB Circular A-130, Management of Federal Information Resources, Appendix I \(http://www.whitehouse.gov/omb/circulars/a130/appendix\\_i.pdf\)](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 staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

### **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.

### **What are the Privacy Act Requirements?**

**Privacy Act.** The [Privacy Act of 1974](http://www.usdoj.gov/foia/privstat.htm), 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.

### **Why is the PIA Summary Made Publicly Available?**

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 Act Officer 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 Single Family Housing

**Subject matter expert in the program area:** Michael Reyes, Management Information Specialist, Office of Single Family Asset Management, Office of Housing, (202) 708-1672

**Program Area Manager:** Ivery Himes, Director, Asset Management & Disposition Division, Office of Housing, (202) 708-1672

**IT Project Leader:** Jeannie Bonifer, Realty Specialist, Asset Management and Disposition Division, Office of Housing, (202) 708-1672

### For IT Systems:

- **Name of system:** Asset Disposition and Management System (ADAMS)
- **PCAS #:** N/A - not WC funded
- **OMB Unique Project Identifier #:** N/A
- **System Code:** P260

### For Information Collection Requests:

- **Name of Information Collection Request:** N/A
- **OMB Control #:** N/A

### Question 1: Provide a brief description of what personal information is collected.

*NOTE: Narrative below is written in present tense, however, P260 is presently in development. Once P260 is in production, narrative would be in proper tense.*

ADAMS supports the major functions that are necessary to manage the day-to-day operations associated with the HUD single-family inventory of properties. The four major functions supported by ADAMS are:

- Acquire Property
- Maintain Property
- Dispose of Property
- Monitor and Report Status of Inventory

ADMS tracks and reports on HUD homes for sale and processes all financial transactions related to their repair, lease, listing, and sale, including payments for contractor services, taxes, and condominium fees. ADAMS tracks, reports, and accounts for homes in HUD's custody. ADAMS is integral to managing the portfolio of HUD homes, acquired at the rate of 50,000 to 70,000 properties per year; monitoring contractor performance; limiting discount programs to eligible participants; and providing management information needed for program oversight and compliance with Congressional, auditor, and other requests.

ADAMS maintains a database of all HUD acquired properties. Initial records are established through a daily interface with the Single Family Claims system (for conveyance claims) or on-line entry by HUD staff (for abandoned homes securing mortgages that have been assigned to HUD or properties foreclosed under the Title I, Section 312 or another agency's program). Management and Marketing (M&M) contractors enter online transactions which updates property status in a real time mode. Properties are tracked through the sales process by monitoring adherence to HUD's disposition requirements and timeframes. Access to property data by HUD staff and contractors is online and interactive. Reports can be created either online or in a batch mode. Historical data is maintained for each property to track sales progress and costs. Inventory activity reports are created monthly. Ad hoc reports are created for special programs and audit agencies as required. Property listing information is created daily. Contractor payments are created monthly and tax data is gathered daily and reported yearly. The purpose of ADAMS is to record all data associated with daily maintenance of case records. ADAMS provides report capabilities for National, Home Ownership Center, and Area/Office management requirements.

System access is granted to M&M contractors engaged in conducting management and marketing services on HUD homes (through them to the real estate industry's Multiple Listing Services). Extracts of HUD homes for sale are posted on HUD's Internet site and kiosks.

Records created in ADAMS remain in the active database until the case record is closed. ADAMS data on closed records are archived.

There are four (4) home ownership centers (HOCs) that support HUD's acquired asset operations. They are located in Philadelphia, Atlanta, Denver, and Santa Ana, and support operations nationwide. HUD uses M&M contractor personnel to administer asset management operations in each HOC area. These contractors are responsible for marketing and management of HUD's single family assets under each HOC's oversight.

This system needs to be protected to assure timely receipt of sales proceeds and rental collections and to prevent fraudulent payments to appraisers, closing agents, brokers, property managers, homeowner/condominium associations, and trade/service vendors.

Messages about system downtimes, key system changes, new process steps, and other alerts are posted on the ADAMS Bulletin Board. HUD management directs the content and timing of the messages. Messages can be posted at any time during the day and can affect processing with the next sign-on to ADAMS. Users should access the Bulletin Board from ADAMS main menu at least twice a day. Checking the Bulletin Board at the beginning and then at end of the day keeps the user abreast of any immediate issues that need attention.

There are approximately 200 ADAMS users at the HQ and 800 users outside the HQ.

Users of ADAMS (online system, batch processes, interfaces, and reports) are:

- Homeownership Centers (HOCs)
- The Housing Office of Finance and Budget
- The Housing Office of Single Family Asset Management

- Management and Marketing contractors

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): <b>Employee Identification Number (EIN) or SSN is mandatory for prospective purchaser and those who do business with HUD in the course of managing and marketing these properties</b>
	Other identification number (specify type):
	Birth date
	Home address
	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
X	Other (specify): <b>Property Address, Business address and phone number</b>
	None
	Comment:

**Personal/ Sensitive Information:**

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

**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"/>

<p>What security controls are in place to protect the information (e.g., encryptions)?</p> <p><i>Data is stored in an Oracle database that is only accessible thru the ADAMS program. ADAMS access requires two levels of logins to access the system. The first login uses to HUD Siteminder system to verify that the user has active HUD authorization. The second login uses ADAMS internal security system to set permissions for data access and system functionality.</i></p>
<p>What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?</p> <p><i>Internet Explorer is used to access the ADAMS.</i></p>
<p>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?</p> <p><i>There is no policy to restrict access. A majority of the users are outside the Department.</i></p>
<p>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)?</p> <p><i>There is no provision in ADAMS for directly downloading data. Reports can be run from the system and saved.</i></p>
<p>Comment:</p>

**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 checked="" type="checkbox"/>	<input type="checkbox"/>
Does the system require authentication?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**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):

X	<b>Conversion:</b> When paper-based records that contain personal information are
---	---

	converted to an electronic system
	<b>From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable):</b> When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
	<b>Significant System Management Changes:</b> 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)
	<b>Merging Databases:</b> 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)
	<b>New Public Access:</b> 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)
	<b>Commercial Sources:</b> 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)
	<b>New Inter-agency Uses:</b> When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	<b>Business Process Re-engineering:</b> When altering a business process results in significant new uses, disclosures, or additions of personal data
	<b>Alteration in Character of Data:</b> 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
X	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u> )
	<p>Comment: Form HUD-9548, OMB Approval No. 2502-0306 (exp. 7/31/2010)</p> <p>Form HUD-9548-b, OMB Approval No. 2502-0306 (exp. 7/31/2010)</p> <p>Form HUD-9548-d, OMB Approval No. 2502-0306 (exp. 7/31/2010)</p> <p>Form HUD-9549, OMB Approval No. 2502-0570 (exp. 2/28/2011)</p> <p>Form HUD-9549-a, OMB Approval No. 2502-0570 (exp. 2/28/2011)</p> <p>Form HUD-9549-b, OMB Approval No. 2502-0570 (exp. 2/28/2011)</p> <p>Form HUD-9549-c, OMB Approval No. 2502-0570 (exp. 2/28/2011)</p> <p>Form HUD-9549-d, OMB Approval No. 2502-0570 (exp. 2/28/2011)</p> <p>Form HUD-9549-e, OMB Approval No. 2502-0570 (exp. 2/28/2011)</p>

--	--

**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
X	Other (specify): <a href="#">Tracking the process of selling HUD Homes</a>
	Comment:

**Rental Housing Assistance:**

	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

**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:

**Internal operations:**

	Employee payroll or personnel records
	Payment for employee travel expenses
X	Payment for services or products (to contractors) – if any personal information on the payee is included
	Computer security files – with personal information in the database, collected in

	order to grant user IDs
	Other (specify):
	Comment:

**Other lines of business (specify uses):**


**Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?**

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):
X	Comment: Information will be shared only with approved HUD Headquarters and HOC staff. HUD contracts with Management and Marketing contractors who support the management, marketing, and disposition of HUD owned real estate. These contractors are required to view and update information in P260 in the course of their daily business.

**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)?**

	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
X	No, they can’t “opt-out” – all personal information is required
	Comment:

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): \_\_\_\_\_

\_\_\_\_\_

**Question 6: How will the privacy of the 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	When an employee leaves: <ul style="list-style-type: none"> <li>• How soon is the user ID terminated? <b>Using the CHAMPS system, generally about 1 week.</b></li> <li>• How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): <b>Notification via CHAMPS</b></li> </ul>
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"> <li>• Full access rights to all data in the system: <b>3 users</b></li> </ul> Limited/restricted access rights to only selected data: <b>Approximately 850 – 1,000 users</b>
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): <b>Electronic files are stored on disc and back up files are stored on tape. All manual files are locked in cabinets when not in use. Computerized files/records are retained until the program office gives direction to archive old cases.</b>
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: <p><b>Datawarehouse, D64A complies with HUD security and privacy requirements</b></p>
	Other methods of protecting privacy (specify):
	Comment:

**Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?**

Mark any that apply

	Name:
	Social Security Number (SSN)
X	Identification number (specify type): <b>Name and Address Identifier (NAID)</b>
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name

	Home address
	Home telephone
	Personal e-mail address
X	Other (specify): FHA Case number, property address (including other geographical characteristics such as contract area, property state/city/county/zip code, Homeownership Center), or contractor ID or name.
	None
	Comment:

**Other Comments (or details on any Question above):**

### **SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER**

ADAMS supports the major functions that are necessary to manage the day-to-day operations associated with the HUD single-family inventory of properties. ADAMS maintains a database of all HUD acquired properties and contains a limited amount of personally identifiable information about the prospective purchaser and those who conduct business with HUD. The system offers equitable administrative controls requires a two levels of log-in for users to obtain system access. It is the policies and procedures and laws that govern the protection of the data that ultimately protect individual privacy rights. The security safeguards, administrative controls, and professionalism applied by ADAMS officials serves to further protect individual privacy rights. This system is also classified as a Privacy Act System of Records (SORs). You may view the published SORs by going to → <http://www.hud.gov/offices/cio/privacy/fedreg.cfm>.