

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

**Office of Single Family Housing, Program
Development, Division of Program
Support**

Nonprofit Data Management System

Privacy Impact Assessment

September, 2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for the Nonprofit Data 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.

Robert Brown

**SYSTEM OWNER, OFFICE OF SINGLE
FAMILY HOUSING, PROGRAM
DEVELOPMENT
[PROGRAM OFFICE]**

09/29/08

Date

Ruth Roman

**PROGRAM AREA MANAGER, DIVISION OF
PROGRAM SUPPORT, RUTH ROMAN
[PROGRAM OFFICE]**

09/23/08

Date

N/A

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

Date

Donna Robinson-Staton

**DEPARTMENTAL PRIVACY ACT OFFICER,
DONNA ROBINSON-STATON**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

10/08/08

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?	6
Why is the PIA Summary Made Publicly Available?	6
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?	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?	11
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	12
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?.....	13
Question 7: 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.....	14

FINAL/APPROVED

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

NONPROFIT DATA MANAGEMENT SYSTEM (NPDMS)

(for IT Systems: N/A and PCAS #: N/A)

September 2008

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 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) (<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: Single Family Housing, Program Development

Subject matter expert in the program area: Tanya Gunn, Program Policy Specialist, Office of Housing, Program Support Division, (202) 708-0317, Extension 2350 and Terri Ames Program Policy Specialist, Office of Housing, Program Support Division, (202) 708-0317, Extension 3025

Program Area Manager: Ruth Roman, Director of the Program Support Division, Office of Housing, Home Mortgage Insurance Division, (202) 708-0317

IT Project Leader:

For IT Systems:

- **Name of system:** Nonprofit Data Management System (NPDMS)
- **PCAS #:** N/A
- **OMB Unique Project Identifier #:** N/A
- **System Code:**

For Information Collection Requests:

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

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

NPDMS collects personal information on board members and key employees of participating nonprofits and homebuyers that purchase HUD Real Estate Owned (REO) Homes from agencies that participate in the REO discount sales program.

NPDMS is an automated web-based program management tool designed to improve the application, recertification, and reporting process for organizations that participate in the Office of Single Family Housing (OSFH) activities and to assist HUD staff with the daily administration of FHA's Nonprofit Program activities.

FHA, through its four Homeownership Centers (HOCs), receives application and recertification packages as well as annual reports from organizations that participate in Office of Single Family Housing (OSFH) activities such as purchasing HUD/REO homes at a discount, providing secondary financing in conjunction with FHA-insured mortgages, and securing FHA loans as the Mortgagor. In the past, participating organizations had to submit the required documents in paper form to FHA. To ease the burden of creating documents, printing them, and mailing them to the HOC, FHA has developed NPDMS. NPDMS will serve as a new means for industry clients to submit data required by FHA.

NPDMS collects, stores and provides web-based access to participants' application and property activity data. This property data includes limited information on homebuyers that purchase HUD

REO properties. The system enhances FHA’s ability to manage an organization’s program activities from initial application/re-certification through the entire life cycle of program activities. Additionally, NPDMS enables participating organizations to: (1) submit required property reports on-line; and (2) access Geographic Information System (GIS) capability and data on HUD-REO properties that are eligible for purchase.

The records maintained in the system are used by HUD staff to: (1) verify an agency’s eligibility to participate in the program; (2) to validate that no conflicts of interest exists amongst board members, employees, business partners, and homebuyers; (3) to validate that discounted HUD REO homes were sold to eligible buyers; and (4) to determine that participating agencies have not exceed profit limits on the re-sale of HUD REO homes purchased through the discount program.

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:

<input checked="" type="checkbox"/>	Name (Name of participating agencies, board members and key staff and program homebuyers)
<input checked="" type="checkbox"/>	Social Security Number (SSN)- (SSN’s of board members and key staff and program homebuyers) only the last 4digits are viewable by HUD staff
	Other identification number (specify type): Agencies EIN numbers are collected
	Birth date
<input checked="" type="checkbox"/>	Home address
	Home telephone:
	Personal e-mail address
	Fingerprint/ other “biometric”
	Other (specify):
	None
	Comment:

Personal/ Sensitive Information:

<input checked="" type="checkbox"/>	Race/ ethnicity
	Gender/ sex
	Marital status
	Spouse name
	# of children
<input checked="" type="checkbox"/>	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):
	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? – No, we are in the process of working with the security office and the contractor to determine what measures can be taken to make sure that the system is meeting all of the departments requirements	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<p>What security controls are in place to protect the information (e.g., encryptions)?</p> <p>UAI further secures the system as part of their normal best practices review of all services. Best practices for software include:</p> <ul style="list-style-type: none"> • Review of all security controls. • Obtain and apply SSL Certificates. • Review URLs to ensure use of HTTPS. • Store passwords in non-human readable format. • Inspect all SQL queries to prevent SQL injection attacks. <p>Server systems are in a secured location with coded key entry for restricted access that has been inspected and approved by HUD.</p> <p>The Public HUD site hosted by UAI is in separate domain from non-profit data management service hosted by UAI.</p> <p>Data is backed up nightly with copies stored in a secure location for disaster recovery.</p> <p>Encryption and hashing techniques are applied to PH information.</p>		
<p>What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?</p> <p>NPDMS is not housed on HUD server/firewall therefore the system does not use a HUD approved application to grant remote access.</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? –Remote access is permitted. However, there is currently not a policy in place that restricts access locations. However, such language to the users guide and the mortgagee letter.</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)? - **There is currently not a policy in place that restricts access locations. However, such language will be added to the users guide and the mortgagee letter.**

Comment:

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? Not other than passwords and user ids.	<input type="checkbox"/>	<input checked="" 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):

<input checked="" type="checkbox"/>	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
	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)
	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)
<input checked="" type="checkbox"/>	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)
	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)

	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
	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
X	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>
	Comment:

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): - To verify that Nonprofits have sold HUD discounted properties to program eligible homebuyers.
	Comment:

Rental Housing Assistance: N/A

	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: N/A

	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: N/A

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

Internal operations: N/A

	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
	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): Identify Conflict of Interest

X	To determine if any conflicts of interest exist between board members, key staff, nonprofit business partners and homebuyers.

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

HUD will not share any person data with other agencies.

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):
N/A	Comment:

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	<p>When an employee leaves:</p> <ul style="list-style-type: none"> How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? Within 24 hours of the agency notifying HUD. For HUD staff within 24 hours after the contractor is formed to disable their password. How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): An area specific system administrator will check NPDMS within 3 days of the employee’s departure to determine if their user account has been disabled in the system.
Yes	<p>Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> Full access rights to all data in the system: Limited/restricted access rights to only selected data: <p>There are approximately 594 authorized users of the system assigned passwords and user ids. For the 594 authorized users, access rights are as follows: 63- Have Internal System Administrator Access (These are HUD Program Management Staff and Contractor Technical Support Staff.) 139 HUD users have general limited access to view agencies information. 392- Non-HUD staff users have access limited to information on their agency only.</p>
Yes	<p>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): Data is backed up nightly with copies stored in a secure location for disaster</p>

	recovery.
N/A	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:
	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

X	Name: Agency information is retrieved by clicking on the name of the agency.
	Social Security Number (SSN)
X	Identification number (specify type): Homebuyer records are retrieved by clicking on a REO Case file numbers.
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.

NPDMS collects SSNs and the TINs of the Non-profit organization board members and key staff and home buyers. The system only contains a limited amount of personal information on the homebuyers. I have determined that the current administrative controls in place for NPDMS are sufficient to ensure protection of the personal information. System access is granted only to staff with a need for such access via the use of a user-id and password.