

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

Office of Housing

**Single Family Housing Enterprise Data
Warehouse (SFHEDW/D64A)
Privacy Impact Assessment**

Updated March 28, 2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Single Family Housing Enterprise Data Warehouse (SFHEDW/D64A)**. 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.

MANAGEMENT ENDORSEMENT

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/ Margaret Burns

MARGARET BURNS
Director, Office of Single Family Program Development
U. S. Department of Housing and Urban Development

04/01/08

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

04/07/08

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	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.....	9
Question 4: Why is the personally identifiable information being collected? How will it be used?	10
Question 5: Will you share the information with others?	11
For Example: another agency for a programmatic purpose, or outside the government.	11
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)?.....	12
Question 7: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	12
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	14

FINAL

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
“SINGLE FAMILY HOUSING ENTERPRISE DATA WAREHOUSE - SFHEDW/D64A”
(for IT Systems: OMB Unique Identifier ?? and PCAS # 00251380)

March 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>); 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?

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.

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 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: Housing, Office of Single Family Housing Program Development
Subject

Subject Matter Expert in the Program Area: Bonnie McCloskey, Program/ Policy Specialist, Home Mortgage Insurance Division, (202) 402.8138

Program Area Manager: Margaret Burns, Director, Office of Single Family Program Development, (202) 402-3989.

IT Project Leader: Sheila Alpers, IT Specialist/SW, Office of Chief Information Officer, (202) 402-7610; Paul E. Theisen, Director, Real Estate Insurance Division, Office of the Chief Information Officer (202) 402-7614

For IT Systems:

- **Name of system:** Single Family Housing Enterprise Data Warehouse – SFDW/D64A
- **PCAS #:** 00251380 **OMB Unique Project Identifier #:**

For Information Collection Requests:

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

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

The Single Family Housing Enterprise Data Warehouse - - The Single Family Housing Enterprise Data Warehouse (SFHEDW/D64A) is an ongoing, fully operational data warehouse that is the key source of data for anyone who needs Single Family FHA mortgage insurance data. SFHEDW is an integrated data warehouse that contains critical Single Family business data from fourteen (14) sources, mostly from FHA Single Family automated systems. The system allows queries and provides reporting tools to support oversight activities, market and economic assessment, public and stakeholder communication, planning and performance evaluation, policies and guidelines promulgation, monitoring and enforcement. The SFHEDW/D64A helps the FHA manage its \$398 billion portfolio of active single-family mortgages.

The Single Family Housing Enterprise Data Warehouse does contain data that is subject to the Privacy Act and the Freedom of Information Act. However this information is restricted, with permission (s) granted by userID. The majority of the tables/ views are accessible to the public group.

Data elements in the SFHEDW that are protected by the Privacy Act are listed below:

case_nbr	FHA Case Number
borr_nm	Borrower Name
coborr_nm	Co-borrower Name (4 times)
prop_addr_strt	Street Address of the Borrower's Property

borr_ssn_tin	Social Security Number of the Borrower
coborr_ssn_tin	Social Security Number of the Co-borrower (4 times)
fico_score	FICO Score (Experian, Equifax and TransUnion)

The following data marts and special tables are maintained in SFHEDW/D64A:

<ul style="list-style-type: none"> ▪ Claims ▪ Default ▪ Default Summary ▪ Integrated Database ▪ Loss Mitigation Portfolio Analysis ▪ Public ▪ SF Assets ▪ Single Family Premium Collection System 	<ul style="list-style-type: none"> ▪ Title I ▪ Home Equity conversion Mortgage (HECM) ▪ Special tables and scoring analysis (Restricted Access) ▪ Appraiser tracking system ▪ Metadata ▪ Single Family Property Disposition
---	---

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
<input checked="" type="checkbox"/>	Social Security Number (SSN).
<input checked="" type="checkbox"/>	Other identification number (specify type): Tax Identification Number
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	Gender/ sex
<input checked="" type="checkbox"/>	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
<input checked="" type="checkbox"/>	Employment history: (only shows if self-employed, and how many years)
	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?

If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
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)? A User ID and password as well as ODBC drivers are required to get through the HUD Lan to the server.		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? VPN and Citrix.		
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)?

If yes, please proceed to answering the following questions.	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
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"/>
Comment: SFHEDW/D64A was developed in 1996		

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):

N/A	Conversion: When paper-based records that contain personal information are converted to an electronic system
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)
N/A	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)
N/A	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)

Note: The SFHEDW merges data from various SF legacy systems which is used to build the Integrated Database (IDB) data mart, which contains the FHA single family portfolio. All data elements protected by the Privacy Act are in multiple systems that feed the warehouse.

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: SFHEDW/D64A became operational in 1996

Question 4: Why is the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

X	Credit checks (eligibility for loans)
X	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
X	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
X	Loan default tracking
X	Issuing mortgage and loan insurance
	Other (specify):
	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)
X	Property inspections – Technical reviews and appraisals are done. We have no way

	of knowing if HUD uses SFHEDW data for Rental Housing Assistance.
	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
	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?

For Example: another agency for a programmatic purpose, or outside the government.

Mark any that apply:

X	Federal agencies? (specify): Census, GNMA, CBO and Archives are several agencies that use SFHEDW data.
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
X	FHA-approved lenders?
X	Credit bureaus?
X	Local and national organizations? FOIA and/or AD Hoc requests
	Non-profits?

	Faith-based organizations?
	Builders/ developers?
	Others? (specify):
X	Comment: We receive written FOIA and Ad Hoc requests through formal HUD channels; FOIA requests come through the SFHEDW Security Administrator(SA). The FOIA office maintains records of each request. If requested data contains Privacy Act data, two extracts are created—one without the Privacy Act data and one including the Privacy Act data. These extracts are placed on separate CDs. The extract with Privacy Act data is compressed, encrypted and password-protected. The CDs are transferred to the Security Administrator by private courier. The FOIA office determines if and how this information can be released.

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)?

X	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: A borrower and/or co-borrower can refuse to list their race; and the lender can list their race based on observance.

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): HUD collects race data for all five borrowers. The borrowers can refuse to list their race... That being said, the lender can list their race based on observance.

Question 7: 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"> How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): See Comment below.
	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 #)? We currently have 641 users, both at HUD Headquarters and in field office locations. Limited/restricted access rights to only selected data (specify #) Approximately 12 users in the Office of Evaluation and PD&R have read only access. Access for FICO Score data is limited, and approval comes from the

	<p>Director of the Office of Evaluation. To gain access to data that is subject to the Privacy Act and/or prohibited from publication under the Freedom of Information Act users must obtain a User ID and password. Personal Data about mortgagors, specifically names, addresses and social security numbers must be protected from unauthorized disclosures. A user ID and password is needed to gain full access to the SFHEDW must complete a User Registration for ADP Resources Form (Form HUD 22017</p> <p>You may access certain data elements that are not subject to the Privacy Act by using the SFHEDW Website (http://hudweb.hud.gov/apps/po/h/sfdw) Query Tool. The query tool only returns summarized date from SFHEDW that has been cleared and released to the general public. No ID or password is required for use of the SFHEDW website</p>
X	<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): Copies of FOIA and/or Ad Hoc request deliverables are retained in a locked file cabinet in a secure wing or a secure building.</p>
X	<p>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: We share information with Neighborhood Watch. Neighborhood is responsible for protecting the privacy of the data and uses the FHA Connection Security module. D64 does not transfer data back to any of the 14 source systems.</p>
	Other methods of protecting privacy (specify):
X	<p>Comment: The SFHEDW does not receive formal notification when an employee leaves and/or terminates. When email correspondence is returned we contact the Security Administrators for HUD and the OIG for Confirmation on termination.</p> <p>When HUD employees leave the agency, their supervisor is supposed to submit a "Revocation"/Removal via CHAMP. The same is true when a contractor stops working on a HUD contract--the GTR is supposed to submit a CHAMP "Revocation" to remove access to applications. One CHAMP request can be used to revoke access to multiple applications, the active directory and email.</p> <p>Additionally, employees are to submit form HUD-58, Clearance for Separation of Employee, part 4 as part of their clearance process to have their privileges terminated. This form is to be Initiate 5 days prior to an employee's separation. When HUD-58-A, "Clearance For Separation of Employee", is signed by IT Security, they make a note of the person and monitor the process of revocation of access.</p>

Question 8: If privacy 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):
X	Birth date
X	Race/ ethnicity
X	Marital status: Borrower Marital Status
X	Spouse name: Coborrower Name (4 times)
X	Home address
X	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

The Single Family Data Warehouse contains read only data from HUD's Legacy systems some of which is subject to the Privacy Act and Freedom of Information Act. However, access to this data is restricted, with permission (s) granted by userID. The majority of the tables/ views are accessible to the public group. Since data in system is sensitive, we will annually monitor this system and related business processes to ensure that adequate privacy protections are in place and will update the applicable PIA as necessary.