

U.S. Department of Housing and Urban Development

Office of Single Family Asset Management Servicing & Loss Mitigation Division (a/k/a National Servicing Center)

Single-Family Mortgage Asset Recovery Technology (SMART)

Privacy Impact Assessment

June 26, 2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Single-Family Mortgage Asset Recovery Technology (SMART)**. 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 T. MORRIS, DIRECTOR, OFFICE OF SINGLE FAMILY ASSET MANAGEMENT, U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

6/30/08

Date

/S/ SHARON LUNDSTROM

PROGRAM AREA MANAGER – SHARON LUNDSTROM, DIRECTOR, OFFICE OF SINGLE FAMILY ASSET MANAGEMENT, SERVICING & LOSS MITIGATION DIVISION (A/K/A NATIONAL SERVICING CENTER)
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

6/28/08

Date

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

7/7/08

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?	8
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?	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)?	12
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: SINGLE-FAMILY MORTGAGE ASSET RECOVERY TECHNOLOGY (SMART)

**(for IT Systems: Insert OMB Unique Identifier: N/A
and Insert PCAS #: N/A)**

June 26, 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) 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 perform 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 seven (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 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 Asset Management Servicing & Loss Mitigation Division

Subject matter expert in the program area: Felicia B. Jones, Branch Chief, Housing, Office of Single Family Asset Management, Servicing & Loss Mitigation Division (a/k/a National Servicing Center), Tulsa, Oklahoma, (918) 292-8958

Program Area Manager: Sharon Lundstrom, Director, Housing, Office of Single Family Asset Management, Servicing & Loss Mitigation Division (a/k/a National Servicing Center), Tulsa, Oklahoma, (405) 609-8443

IT Project Leader: Felicia B. Jones, Branch Chief, Housing, Office of Single Family Asset Management, Servicing & Loss Mitigation Division (a/k/a National Servicing Center), Tulsa, Oklahoma, (918)292-8958; Sally Bene`, Program Director-Servicing, Housing, Office of Single Family Asset Management, Servicing & Loss Mitigation Division (a/k/a National Servicing Center), Tulsa, Oklahoma, (918)292-8957

For IT Systems:

- **Name of system:** Single-Family Mortgage Asset Recovery Technology (SMART)
- **PCAS #:** Not Applicable
- **OMB Unique Project Identifier #:** Not Applicable.
- **System Code:** A80H

For Information Collection Requests:

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

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

The SMART System is a loan servicing system used to provide various levels of service for single family home loans. It provides full service to Home Equity Conversion Mortgages (HECM) mortgages assigned to HUD and Secretary Held loans. It provides limited servicing for various other loans and acts as a custodian and provides release and limited servicing to still other loans. SMART is used to provide servicing to 9 different types of loans. To service these loans, the information checked below is needed to identify the borrower and the property.

HECM INSURED
HECM ASSIGNED
PARTIAL CLAIMS
GOOD NIEGHBOR NEXT DOOR

SECRETARY HELD (old assignment program)
 235 INSURED
 NEHIMIAH
 ACA ENFORCEMENT/COMPLIANCE
 ACA PMM

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

Personal Identifiers:

X	Name
X	Social Security Number (SSN).
X	Other identification number (specify type): FHA Case Number
X	Birth date
X	Home address
X	Home telephone
X	Personal e-mail address
	Fingerprint/ other "biometric"
X	Other (specify): Alternate phone numbers, POA'S
	None
	Comment:

Personal/ Sensitive Information:

	Race/ ethnicity
	Gender/ sex
X	Marital status
X	Spouse name
	# of children
X	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Bank account number
	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? If yes, what security controls are in place to protect the information e.g., encryptions (give details below)?

	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 type="checkbox"/>	<input checked="" type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)? Password protection on both the system/database and network. Network credentials are required to enter the system/database. Data is not encrypted but the system/database login and password are encrypted. Physical security measures are in place to limit physical access to authorized individuals (see SMART System Security Plan).		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? The SMART System is housed on servers maintained and secured by contracted services , C & L Service Corporation and Morris-Griffin Corporation. The system is remotely accessible by designated HUD employees through the web based CITRIX system. The access for HUD users is limited to reading the information in the system and making notes. There are two login and password combinations to access the system from outside the physical Morris-Griffin premises, the first to the CITRIX system and secondly to the SMART system.		
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? No. There is not a policy in place to restrict remote access to certain locations.		
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)? No. There is not a policy in place to restrict downloading and remote storage.		
Comment:		

Question 3: Type of electronic system or information collection.

Fill out Section A, B, or C as applicable.

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

	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 type="checkbox"/>	<input checked="" type="checkbox"/>
Is the system external-facing (with external users that require authentication)? No, only authorized system users (as determined by the GTR) are allowed to access the system. These users are not granted access beyond the HUD firewall.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Comments: The SMART System has been available to HUD employees online since its implementation in 2004. It is accessed through the web based CITRIX system that requires a unique login and password combination and the SMART system itself which requires a separate login and password combination for access.

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):

The items marked “N/A” are not required for our area of loan servicing.

X	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
X	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new “relational” databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
X	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
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)
X	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
X	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

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

	Yes, this is a new ICR and the data will be automated
X	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
N/A	Comment: <u>The SMART System automated and replaced an existing, manual system, so the information used is not new.</u>

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

Mark any that apply:

Homeownership:

X	Credit checks <u>Credit checks are performed on a limited population of loans for loss mitigation – i.e. forbearance plans</u>
	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 <u>Loans moving through the default process are tracked by steps to insure foreclosure actions are progressing in accordance with the timeline requirements and/or loss mitigation is being offered timely.</u>
	Issuing mortgage and loan insurance
	Other (specify):
	Comment: <u>The information required and used by SMART is for the purpose of servicing various loans, and tracking those in default. This is a standard loan servicing operation. The items not marked do not apply to our area of loan servicing.</u>

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:

<input type="checkbox"/>	Housing discrimination complaints and resulting case files
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Internal operations:

<input type="checkbox"/>	Employee payroll or personnel records
<input type="checkbox"/>	Payment for employee travel expenses
<input type="checkbox"/>	Payment for services or products (to contractors) – if any personal information on the payee is included
<input type="checkbox"/>	Computer security files – with personal information in the database, collected in order to grant user IDs
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Other lines of business (specify uses):

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

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:

<input checked="" type="checkbox"/>	Federal agencies?
<input type="checkbox"/>	State, local, or tribal governments?
<input type="checkbox"/>	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
<input checked="" 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):
<input type="checkbox"/>	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)?

<input type="checkbox"/>	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: generated for system Alphanumeric 6-8 characters including 1 special character
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): Policies and procedures are in place to ensure that a terminated employee's network and system access are removed immediately. This process is initiated by the completion and submission of a form by the terminated employee's immediate supervisor. More details are available in the SMART System Security Plan.
YES	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: 49 contractor staff users have general, full access (SMART Main), 2 have access as financial management with the ability to produce checks (SMART Fin Mgmt), 5 are designated generally as management (SMART Mgmt) and 4 are assigned to the programmers group (Programmers), which has full access (two of the Programmer users are actually assigned to system process accounts, not actual individuals). • Limited/restricted access rights to only selected data: 65 HUD users are given read only access to the system. The vast majority of these users are HUD employees. The access for HUD users is limited to reading the information in the system and making notes.
YES	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): Electronic files are stored on servers and back up files are stored on tapes. Servers are stored in a secured server room and at an offsite secured facility for disaster contingency. The original collateral documents (hard copy) are stored at the Contractors office site for all open loans and the closed documents are stored at a secured offsite document storage facility. All hard copy files are stored within a secured room within the Contractor's secured office suite when not in use.

NO	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: Last Name
X	Social Security Number (SSN)
X	Identification number (specify type): FHA Case Number
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
X	Home address
	Home telephone
	Personal e-mail address
X	Other (specify): ALTERNATE PHONE NUMBER
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

SMART is a loan servicing system used by Housing’s Office of Single Family Asset Management Servicing & Loss Mitigation Division. SMART provide various levels of loan servicing functions for single family home loans. The system offers equitable risk assessment using a secure encrypted network for system access; however, 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 SMART 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 full text of the published SORs by going to → <http://www.hud.gov/offices/cio/privacy/fedreg.cfm>.