U.S. Department of Housing and Urban Development

Office of Housing

Single Family Insurance System
(CLAIMS) Sub-System

Privacy Impact Assessment

September 2005

Document Endorsement

I have carefully assessed the Privacy Impact Assessment (PIA) for Single Family Insurance System-CLAIMS Subsystem. 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.

X **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/ Eric M. Stout — **Dec. 15, 2005**
Departmental Privacy Advocate — **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

/s/ Jeanette Smith — **Dec. 15, 2005**
Departmental Privacy Act Officer — **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

TABLE OF CONTENTS

FINAL/ APPROVED

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
"SINGLE FAMILY INSURANCE SYSTEM-CLAIMS SUBSYSTEM"
(for IT Systems: OMB Unique Identifier 025000101020000000206085
and PCAS # 0000251080)
October 2007

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 Handbook1325.1 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 superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security

regulations at Title 44 U.S. Code chapter 35 subchapter II (http://uscode.house.gov/search/criteria.php); and

- OMB Circular A-130, Management of Federal Information Resources, Appendix I (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those 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 8 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, 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, 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 Financial Services
Subject matter expert in the program area: Sarah Martin, Chief, Single Family Claims Branch, Office of Housing, 202-402-3225
Program Area Manager: James R. Curry, Director, Single Family Post Insurance Division, 202-402-3297
IT Project Leader: Chuck Yoshida, Computer Specialist, Office of the Chief Information Officer, Office of Systems Integration and Efficiency, 202-402-7603
Sheila Alphers, Computer Specialist, Office of Chief Information Officer, Office of Systems Integration and Efficiency, 202-402-7610.

For IT Systems:

- **Name of system:** Single Family Insurance System -- Claims Subsystem
- **PCAS #:** 00251080 **OMB Unique Project Identifier #: 025000101020000000206085**

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 Insurance System - Claim Subsystem provides automated receipt, tracking and processing of form HUD-27011, Application for Single Family Mortgage Insurance Benefits. It also provides on-line update and inquiry capability to the Single Family Insurance and Claims databases and to cumulative history files. On a daily basis, claim payment authorizations are sent to Treasury (IBM mainframe /Treasury interface) for disbursement via Treasury's "Automated Clearing House" feature (electronic funds transfer). This process is further automated by providing mortgagees daily Advice of Payment (AOP) and Title Approval letters, using a computerized bulk mail facility and HUD's Electronic Data Interchange (EDI) facility. Claims can come in via EDI (Claim Types 01-07 except Type 05); keypunch (Claim Types 01-07 and 31-33); and FHA Connection (FHAC) (Claims Types 01, 07, 31, 32, and 33

The Office of Financial Services has responsibility for and control of CLAIMS. HUD management has established personnel security policies and procedures to limit access to the processes within the application to those with a need for such access. There is an automated workflow process for requesting, establishing, and issuing user accounts. A user submits a User Registration for ADP Resources, HUD Form 22017, to request access to CLAIMS. Due to sensitivity of the data, a background check is also required for access to CLAIMS. Once the appropriate security screening forms are submitted, access is granted. It can take from 12 to 18 months for completion of the background check. An email message from a supervisor is used to request a change or termination of access. As part of out-processing, for both friendly and

unfriendly terminations, employees must checkout with IT Security to close their user account. In addition, the CLAIMS Security Administrator conducts a quarterly re-validation of users that is forwarded to IT Security to ensure invalid user accounts are closed. Computer Associates-Top Secret (CA-Top Secret) security package implemented on the mainframe computer system requires users to log-on prior to accessing the system. Each CLAIMS user has been assigned a 6-digit user identification (ID), starting with an "H" (for HUD employee) or "C" (for contractor). Under this standard security, users will use the same user ID and password for access to the CLAIMS subsystem. The procedures for granting access to CLAIMS is allowed only with express approval of the Insurance/Claims Branch Chiefs or designated claim staff member. Field staff personnel are limited to inquiry access only. Direct system access is controlled by specific screen and level of access to individual screens. Therefore, it is possible to limit access to only those parts of the system needed. CLAIMS end users having direct access include:

- CLAIMS staff – inquiry and update capability
- Contractors working for CLAIMS Branch – inquiry, restricted data entry
- Other Department staff and field offices – inquiry only
- Current HITS Operations Contractor – Custodian of all physical data files.

Access to FHAC information about claims is controlled by IDs linked to specific companies. Only case data related to a specific company is available to a user under this ID. Although the servers and database are located at the HUD Computer Center, computer room technicians do not have direct account access to CLAIMS software or its data. At the Disaster Recovery Facility (DRF), background screenings are routinely conducted for all new hires before they are granted access to the computer room and system; this screening process has been in place since 2001.

Access to the computers and sensitive software is controlled by user IDs and passwords. Read/write keys also control the production environment. Positions are not reviewed for sensitivity level. Presently there is no planned date for completion of position sensitivity analysis.

The mechanisms in place for holding users responsible for their actions are an audit trail of user actions and the capability to remove access or terminate their user ID. CLAIMS access is removed by the CLAIMS Security Administrator

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
	Birth date
X	Property address
	Property telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	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: all other categories are "not applicable"

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

Yes	No	If yes, what security controls are in place to protect the information e.g., encryptions (give details below)?
☐	☐	If yes, have the security controls been reviewed and approved by the Information Security Officer?
		Not applicable, no personally identifiable information is collected in the system.
		Comment:

Question 3: Type of electronic system or information collection. If a new electronic system (or one in development):

Yes	No	
☐	☒	Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?
☒	☐	a. Does the system require authentication?
☐	☒	b. Is the system browser-based?
☐	☒	c. Is the system external-facing (with external users that require authentication)?
		Comment: A43C has been in operation since March of 1983.

A. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

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 new 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)

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 new or automated)
	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): FHA Claim Payments on FHA-Insured Loans
	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
	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): Fannie Mae, Ginnie Mae, Department of Justice, Treasury, and other FHA Systems
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
X	FHA-approved lenders?
X	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
X	Others? (specify): (CAIVRs)
	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 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: • How soon is the user ID terminated? A user's ID is terminated on the day they check out with ADP Security. (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): The Claims Branch requests advance notice of employee departure and submits a request to the System Security Officer (SSO) to terminate the employee's system access. The SSO confirms that a termination request has been completed.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: • Full access rights to all data in the system: 1 User • Limited/restricted access rights to only selected data: 1050 Users Limited Read Only: 1000 Users Limited Read/Update: 50 Users
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): No disks (except those within PCs), tapes, or hardcopy printouts are maintained. Printouts are normally viewed in softcopy. Any papers containing sensitive data are in locked offices and shredded when no longer needed.
X	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: The receiving system security officer.
	Other methods of protecting privacy (specify):
	Comment:

Question 8: If <u>privacy</u> information is involved, by what data elements can it be retrieved?

Mark any that apply:

X	Name:
	Social Security Number (SSN)
X	Identification number (specify type): FHA Case Number
	Birth date

	Race/ ethnicity
	Marital status
	Spouse name
X	Property address
	Property telephone
	Personal e-mail address
X	Other (specify): Servicer ID and Holder ID
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

The CLAIMS system provides on-line updates and inquiry capability to the Single Family Insurance and Claims databases and to cumulative history files. Due to the sensitive nature of the data transferred and/or contained in CLAIMS a background check is required prior to being granted access to the system and access is given only to staff with a need for such access. Once the appropriate security screening forms are submitted and approved, access is granted.

In November of 2007 a Privacy Act System of Records was published in the Federal Register for F42D and minor updates were applied to the PIA by the System Owner. The updates provide additional clarification concerning the userability of PII data and can be reviewed by referring to questions 2, 3, 5, and 8.