U.S. Department of Housing and Urban Development

Office of Housing

FHA Connection

Privacy Impact Assessment

August 8, 2006

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **[Insert Name of IT System and/ or Information Collection Request]**. 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.

__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/ Margaret E. Burns — **8/9/06**
SYSTEM MANAGER — **Date**
Office of Single Family Program Development

/s/ Richard J. Bradley — **8/9/06**
PROGRAM AREA MANAGER — **Date**
Office of Home Mortgage Insurance Division

_______________________________ ___________

_______________________________ ___________
DEPARTMENTAL PRIVACY ADVOCATE — **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

/s/ Jeanette Smith — **9/6/06**
DEPARTMENTAL PRIVACY ACT OFFICER — **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

TABLE OF CONTENTS

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
"FHA CONNECTION - - FHAC – F17C"

(OMB Unique Identifier 025000102011040002060885 and PCAS # 2516810)

August 2006

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 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, 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: Office of Housing – Office of Single Family Program Development
Subject matter expert in the program area: Richard J. Bradley, Housing Program / Policy Specialist, Office of Housing, Mortgage Insurance Division (202) 708-2121 ext. 2326
Program area manager: Margaret E. Burns, Director, Office of SF Program Development
IT Project Leader: Matthew R. McCants, IT Specialist, Office of the Chief Information Officer, Office of Systems Integration & Efficiency, (202) 708-1587 ext. 7608;
Paul E. Theisen, Director, Real Estate Insurance Division, Office of the Chief Information Officer, Office of Systems Integration & Efficiency, (202) 708-1587, Ext. 7614

For IT Systems:

- **Name of system:** FHA Connection - - FHAC
- **PCAS #:** 2516810
- **OMB Unique Project Identifier #:** 025000102011040000206085
- **System Code:** F17C

For Information Collection Requests:

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

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

FHA Connection is an interactive system available through the Internet that gives approved FHA lenders real-time access to FHA systems for the purpose of conducting official FHA business in an electronic fashion. Users can gain access to the FHA Connection through any browsers that support the Secured Socket Layer (SSL) transmission protocol. SSL is one component of the overall security of the system.

The FHA Connection resides on HUD's Enterprise Server. As of May 18, 2006, 46,468 users from 17,395 institutions and branches have signed up to use the Connection and average volume between 100,000 and 150,000 transactions per day.

Single Family business that is currently supported by FHA Connection System includes: FHA Single Family Mortgage Insurance Underwriting, Single Family Default Reporting, and Portfolio Downloads for the Single Family Periodic Premium Collections System. Transactions correctly submitted through the FHA Connection are ultimately processed on the F17 CHUMS, SFPCS-U, SFPCS-P, F42D, A43C, A43I, F51, MDDR, PASS, and Neighborhood Watch, A80R/P, and the Single Family Default Reporting System. Links are also provided to Hi-cost county limits, appraiser lists and other related links that are available to the public under the HUD Home Page.

FHA loan data are submitted for review and insurance through the FHAC to the Computerized Homes Management Underwriting System (CHUMS). Lenders must submit potential loan recipients' case information to obtain HUD "endorsement" (underwriting approval) of FHA mortgage insurance.

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):
X	Birth date
X	Home address
	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
X	Comment: FHA loans require borrowers to provide personal information sufficient to qualify for a home loan.

Personal/ Sensitive Information:

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

Question 2: 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)? If yes, fill out subsections a, b, and c.

	Yes	Yes	No
	a. Does the system require authentication?	□	□
	b. Is the system browser-based?	□	□
	c. Is the system external-facing (with external users that require authentication)?	□	□
X	No		
	Comment		

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):

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

Mark any that apply:

Homeownership:

	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)
	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
X	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 4: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
X	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):
X	Comment: This information is not shared with other agencies.

Question 5: Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

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

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): ____

____

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password
X	When an employee leaves: • 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): The users are deleted from the systems administrators list.
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 (specify #)? Limited/restricted access rights to only selected data (specify #)? The FHA Connection issues two distinct types of user ids to lenders: Application Coordinators and Standard Users. An Application Coordinator id can perform all functions that a Standard User can perform. In addition, an Application Coordinator is responsible for maintaining the user profiles for all individuals in the Application Coordinator's lending institution. The Application Coordinator is able to access an FHA Connection ID administration screen. The Application Coordinator is then able to grant or revoke access to any and all screens in the FHA Connection to any individual who has a user ID assigned to the Application Coordinator's lending institution. All Application Coordinator's are approved by the CEO of the lending institution.
	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):
	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:
X	Other methods of protecting privacy (specify): • The System Layer provides two types of security. The FHA Connection employs Secure Socket Layer (SSL) to encrypt the data as it is transferred over the Internet. SSL is the industry standard for data encapsulation to ensure secure data transfer. The FHA Connection uses Lightweight Directory Access Protocol (LDAP) for user authentication. SSL is also the industry standard for authentication. A user must be authenticated before the Web server will allow access to any restricted resource. The user must be in the proper LDAP group to be granted access to the requested resource. • The Application Layer provides user authorization. The Application Layer ensures that the user has been granted access to the screen by his Application Coordinator. It also ensures that the particular loan that he is trying to access is owned by his lending institution. The Application Layer will not grant access to loans that are not associated with the user's institution.
	Comment:

Question 7: 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	Other identification number (specify type): FHA Case Number
X	Birth date
X	Home address
	Home telephone
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
X	Comment: Data in the FHA systems is not retrievable by a number that is unique to an individual. The FHA Case Number retrieves it.

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

FHA Connection provides approved FHA lenders real-time access to FHA systems for the purpose of conducting official FHA business in an electronic fashion. The system supports the business and transactions of several of HUD’s legacy systems.

Since FHA Connection does collect personal identifiable information from borrowers to qualify for home loans; therefore, it is critical that adequate security and administrative controls are in place. In reviewing Question 6 above, we have determined that the two type security features are adequate enough to ensure protection of PII.