U.S. Department of Housing and Urban Development

Office of Chief Financial Officer

HUD's Consolidated Financial Reporting System (HCFRS) A39

Privacy Impact Assessment

April 11, 2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **HUD's Consolidated Financial Reporting System (HCFRS) - A39**. 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/ Garland J. Reid — 4/14/08

GAIL B. DISE, SYSTEM OWNER — **Date**
Assistant Chief Financial Officer for Systems
Office of the Chief Financial Officer
U.S. Department of Housing and Urban Development

/s/ Alice B. Cullom for Cherryl Cornelious — 4/11/08

CHERRYL P. CORNELIOUS, SYSTEM ADMINISTRATOR — **Date**
Financial Systems Maintenance Division
Office of the Assistant Chief Financial Officer for Systems
U.S. Department of Housing and Urban Development

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

/s/ Donna Robinson-Staton — 4/15/08

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

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? 10
Question 5: Will you share the information with others? 11
Question 6: Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use 12
Question 6: How will the privacy of the information be protected/secured? 12
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system? 13

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER **13**

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

HUD's Consolidated Financial Reporting System (A39)

(for IT Systems Insert OMB Unique Identifier #: N/A
and PCAS: 00202620

April 11, 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 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 the Chief Financial Officer
Subject matter expert in the program area: Cherryl P. Cornelious, Systems Administrator, Financial Systems Maintenance Division, Office of the Assistant Chief Financial Officer for Systems, (202) 402-3742
Program Area Manager: Gail B. Dise, Assistant Chief Financial Officer for Systems, Office of the Chief Financial Officer, (202) 402-3749
IT Project Leader: Harry S. Laggah, IT Government Technical Monitor (GTM), Office of Systems Integration & Efficiency, OCIO, (202) 402-3752

For IT Systems:

- **Name of system:** A39 HUD's Consolidated Financial Reporting System
- **PCAS #:** 00202620
- **OMB Unique Project Identifier #:**
- **System Code:** HCFRS A39

For Information Collection Requests:

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

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

HCFRS manages financial information inquiries, reports, and reporting to central agencies. This system is HUD's financial reporting system for the consolidation of the general ledger activities from HUD Offices to include the Federal Housing Administration (FHA), Office of Federal Housing Enterprise Oversight (OFHEO), and Government National Mortgage Association (GNMA).

HCFSS provides the following benefits to the Department: timely, complete, and comparable financial reports to OMB; centralizes and provides uniformity in financial information and reporting; complies with Standard General Ledger requirements and Generally Accepted Accounting Principles.

There is no personal information collected by this system.

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:

	Name
	Social Security Number (SSN) .
	Other identification number (specify type):
	Birth date
	Home address
	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
X	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:

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

	Yes	No
If yes, Proceed to answering the following questions.	☐	☒
Have the security controls been reviewed and approved by the Information Security Officer?	☐	☐
What security controls are in place to protect the information (e.g., encryptions)?		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?		

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?
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)?
Comment: N/A: There is no personal information accessed remotely or physically available in system.

Question 3: What Type of electronic system or information collection is your project?

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.	☐	☒
Does the system require authentication?	☐	☐
Is the system browser-based?	☐	☐
Is the system external-facing (with external users that require authentication)?	☐	☐

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)

B. 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
	No, the ICR does not require a PIA because it is not new or automated)
X	Comment: N/A

Question 4: Why is the personally identifiable information being collected? How will it be used? N/A There is no personally identifiable information being collected by this system.

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
	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
	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? (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?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):

X	Comment: HUD's consolidated financial quarterly statement is shared with Treasury and OMB.

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
	No, they can't "opt-out" – all personal information is required
X	Comment: There is no personally identifiable information being collected by this system.

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 The application requires User ID and encrypted passwords to provide authorized users with access. Passwords are changed periodically and rules for length, composition (uppercase/lowercase, numeric) and re-use are dependent upon the individual application controls.
X	When an employee leaves: • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? As part of the employees exit process the security officer sign the forms and removes the employees access ability form the system with in **1 day** of notice. • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): There is an automated workflow process for requesting, establishing, and issuing user accounts. As part of out-processing, for both friendly and unfriendly terminations, employees must checkout with ADP Security to close their user account. In addition, the OCFO security administrator conducts a quarterly re-validation of users that is forwarded to ADP Security to ensure invalid user accounts are closed.
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: (2) • Limited/restricted access rights to only selected data: (20) Users are assigned to groups that are established with certain levels of access. This will prevent users from accessing areas not assigned to that group. The OCFO may

	grant system access to employees, contractors, clients/customers, and program participants who have a need to utilize CFO major application systems. Users must submit a CHAMP request for access to the HUD network, User Request for ADP Resources and form 22017 to request access to OCFO System Applications. Supervisors and the System Security Administrator for appropriate sensitivity level have reviewed all positions. The separation of duties requirement also establishes which level of access an employee will receive.
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): There is no personal or sensitive information captured in the system; however, there is a process in place to protect the security of the sponsor business information.
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: There is no data sharing with another system.
	Other methods of protecting privacy (specify):
	Comment:

Question 7: If <u>privacy</u> information is involved, by what data element(s) is it retrieved from the system?

Mark any that apply

	Name:
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
X	None
	Comment: There is no privacy information retrieved by this system.

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

Based on the assessment of this PIA it is determined that the **Consolidate Financial Reporting System** is not a potential risk warranting privacy protection, because it does not collect, contain, use or disseminate any personal identifiable information.